A Technical Solution to Implement Financial Regulation Into Secondary Markets of Tokenized Financial Assets*

Marcelo Salhab Brogliato[1]
Bruno Ramos Campana[2]
Yan Martins[3]

Abstract

In this paper, we propose a technical solution to implement financial regulation into secondary markets of tokenized financial assets. This solution may assist entities in transitioning their financial market infrastructures from legacy systems to DLT platforms. We conceived the solution for a context where one wants to keep the current financial regulatory framework working, and a central authority has the final word. The main design points of the solution are as follows: (i) financial regulation is implemented as an off-chain layer; (ii) the three roles of this market are token issuers, investors, and a single central authority; (iii) the core component to implement such solution is a feature of DLTs called 'multi-signature wallet'; and (iv) using multi-signature wallets one creates a signature scheme that makes possible the financial regulation compliance of all transactions added to the ledger. After presenting the solution, we explain why we decided to use an off-chain layer rather than an on-chain layer using smart contracts. The main reason for this design decision is that because we have a central authority, most of the benefits of encoding financial regulation into smart contracts are drained. Thus, the disadvantages of an on-chain layer outpace the benefits. An off-chain regulation layer allows the compliance of the solution with the current financial regulatory framework, avoids legal risks, keeps the main benefits of using DLTs, provides agility to adapt and evolve, and makes possible a smooth yet progressive movement to implement DLT into the financial market infrastructure. For all these reasons, we conclude that an off-chain regulation layer brings the optimal solution for the given context.

Keywords: *blockchain;* DLT*; tokenization; financial assets tokenization; financial market infrastructure; regulated decentralized finances; secondary markets; financial regulation.*

The views expressed in this paper are those of the authors and do not necessarily reflect those of the Banco Central do Brasil.do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

* Article submitted to the Bacen workshop on May 16, 2023, in the thematic sub-axis of information technology, in the topic of financial assets tokenization, subtopic: financial market infrastructures based on distributed ledger networks.
fgrinberg@IMF.org
1 Hathor Labs, msbrogli@hathor.network
2 Hathor Labs, bruno@hathor.networ
3 Hathor Labs, yan@hathor.network

1 Introduction

Over the last few years, the financial industry has understood the innovative potential of distributed ledger technologies (DLT) to improve financial markets infrastructure, notably for the transformation of payment, clearing, and settlement processes (PCS) (Mills *et al.*, 2016). Moreover, the most prominent use case of DLTs in the financial industry has become the tokenization of assets (OECD, 2020).

Tokenization of assets is the representation of assets as tokens on a DLT (OECD, 2021). Virtually any asset, either physical or not, can be tokenized: securities (e.g., stocks and bonds), commodities (e.g., gold), real estate properties etc. (OECD, 2020). Some of these assets may belong to financial markets, which can be primary or secondary. The primary market of tokenized financial assets comprises selling new issuances by the issuer (e.g., for raising capital). In turn, the secondary market of tokenized financial assets comprises the trading among investors (Fabozzi, 2009). In this context, one of the technical problems to be solved is: how to implement the due financial regulations of primary and secondary markets of tokenized financial assets over DLTs? (OECD, 2021).

This problem is more prominent in the case of secondary markets. First, for their very nature. Second, because of the removal of many financial intermediaries that take place once using a DLT — and were once accountable for implementing financial regulations. The solution that has been most discussed to address this issue is to encode financial regulations into smart contracts (Momtaz, 2021).

In this paper, *we propose an alternative solution to implement financial regulations into secondary markets of tokenized financial assets*. We argue that our solution is simpler yet more efficient than encoding financial regulations into smart contracts. Furthermore, with this solution, we aim to collaborate to improve the **financial markets infrastructure based on DLT**. Note, however, that we propose a technical solution to be used with pre-existing financial regulations, either in the context of the traditional financial industry (based on DLTs) or decentralized finance (DeFi). Thus, our solution assists in implementing, but not creating new financial regulations for the DeFi niche — for example, to solve the problems of accountability of issuers, jurisdiction definition, geographic uncertainty etc. (OECD, 2022).

This paper is organized as follows. In section 2, we model the problem we intend to solve. In section 3, we design our alternative solution to address the problem. In section 4, we discuss the presented solution vis-à-vis the other alternative. In Section 5, we discuss the solution implications for choosing a DLT platform. Finally, in section 6, we conclude the paper by presenting relevant remarks about the solution.

2 Problem: Implementing Financial Regulation Over a DLT

In this section, we model the problem we intend to solve: implementing financial regulation on a secondary market based on DLT.

2.1 The challenge to translate financial regulation into engineering requirements

Financial regulation is the set of rules that market participants must comply with while participating in market activities. It encompasses the mechanisms of enforcement to deal with non-compliant behavior (on behalf of the participants); it can be handled by either government or non-government organizations (OECD, 2010). Also, financial regulations have three broad goals: (i) prevent the use of funds for illicit activities, money laundering, or tax evasion; (ii) protect participants in financial markets against fraud and abuses; (iii) and ensure the integrity of markets and payment systems and overall financial stability (Makarov; Schoar, 2022).

To do this, financial regulation needs to address multiple issues of financial markets, such as licensing and authorization (*e.g.*, who should be able to issue securities and who should be able to invest); prudential supervision (*e.g.*, anti-money laundering – AML – and countering the financing of terrorism and proliferation – CFT); transparency (including transaction tracking and disclosure of costs and fees); consumer protection and protection of customer funds; transaction limits; foreign exchange regulations; cross-border provision of services; capital controls; sanctions regimes; tax reporting requirements. Furthermore, conflicts of law rules emerge in a cross-border setting (i.e., among different jurisdictions) — for example, jurisdiction *A* prohibits conduct permitted in jurisdiction *B*. Or *A* establishes requirements that are incompatible with the institution's setup in *B* (Zetzsche *et al.*, 2022).

With this non-exhaustive list of examples, we can see the high level of complexity that a **financial regulatory framework** may have in a given jurisdiction. To translate our problem into a list of engineering requirements, we need a way to address such complexity. Our best alternative is to focus not on the rules themselves but on the mechanisms used for compliance and enforcement of a general regulatory framework. In other words, we seek the principles to implement a financial regulatory framework.

2.2 Principles to implement a financial regulatory framework

We can find these principles in publications such as "Objectives and Principles of Securities Regulation" from the International Organization of Securities Commissions (IOSCO, 2003). Although this publication is focused on defining a financial regulatory framework for a specific financial instrument — namely, securities — it suits our needs well. This is because the tokenization of securities has been seen by the market as the most promising niche and also the one that has been with more momentum (OECD, 2020). Also, because securities regulation is a complex subcase that yet has sound legislation throughout the world that we can use as a basis (e.g., IOSCO, 2003; BIS; IOSCO, 2012; BIS, 2017). Thus, we will use securities regulation standards as a proxy for regulating all financial instruments.

Notwithstanding, before using the aforementioned publications, we must ensure that the change of technology — namely, the use of DLT — does not invalidate such principles. Acording to the OECD (2021):

> Regulators in most jurisdictions with active tokenized markets have adopted a technology-neutral approach to policies around tokenized assets and their markets, with the same rules applying to the same activities and risks, irrespective of the technological medium through which the product/service or activity is provided. As such, the use of DLTs or other technology does not affect how these regulators assess whether or not the ensuing financial product/service or activity falls within the regulatory perimeter and, consequently, whether it is regulated or unregulated. (OECD, 2021, [s./p.])

Thus, given the technological neutrality that has been used in most jurisdictions, we can indeed use securities regulation standards to obtain the principles of financial regulation in the context of DLT-based financial market infrastructure (BIS; IOSCO, 2012).

We start defining the market participants relevant to the financial regulatory process. For our purposes here, we need to define three participants (IOSCO, 2003):

- Investors: include all customers or other consumers of financial services.
- Issuers: those who raise funds on the market.
- Regulators: all organizations of a given jurisdiction — either government or non-government — engaged in the financial regulatory process. It goes from policymakers to law courts.

The publication "Objectives and Principles of Securities Regulation" (IOSCO, 2003) sets out 30 principles of securities regulations. From there, we will highlight those that are relevant to our context. There are three *principles for the enforcement of securities regulation* (IOSCO, 2003, p. i):

- Principle 8: The regulator should have comprehensive inspection, investigation and surveillance powers.
- Principle 9: The regulator should have comprehensive enforcement powers.
- Principle 10: The regulatory system should ensure an effective and credible use of inspection, investigation, surveillance and enforcement powers and implementation of an effective compliance program.

The use of DLT is part of the 'regulatory system' cited in principle 10. To these principles, we add the following statements. Regarding the powers and resources of the regulator (IOSCO, 2003, p. 10): "The regulator should have adequate powers, proper resources and the capacity to perform its functions and exercise its powers." In our context, this means that our solution must provide the resources for the regulator to exert its powers over the DLT environment. The following statements clarify the comprehensive enforcement powers of the regulator (IOSCO, 2003, p. 15): "Power to order the suspension of trading in securities or to take other appropriate action. [...]. Where enforcement action is able to be taken, the power to enter into enforceable settlements and to accept binding undertakings." The powers should also cover anti-money laundering (AML) (IOSCO, 2003, p. 16): "The regulator should also require that market intermediaries have in place policies and procedures designed to minimize the risk of the use of an intermediaries business as a vehicle for money laundering."

From the six principles for the secondary market, we highlight here three that are relevant to our problem (IOSCO, 2003, p. iii):

- Principle 25: The establishment of trading systems including securities exchanges should be subject to regulatory authorization and oversight.
- Principle 27: Regulation should promote transparency of trading.
- Principle 30: Systems for clearing and settlement of securities transactions should be subject to regulatory oversight, and designed to ensure that they are fair, effective and efficient and that they reduce systemic risk.

2.3 Engineering requirements to implement a financial regulatory framework

Based on these principles, we will model the functional requirements of our solution. Moreover, there are also some relevant aspects that we will add to model the non-functional requirements. The solution needs to be able to evolve over time (the extensibility) (Árvai; Heenan, 2008, p. 27): "The legal and regulatory framework needs to be continuously adapted to changes in the primary and secondary market infrastructure, participants, instruments, payment and settlement process. The authorities should promote industry bodies that deal with transaction conventions or business conduct standards.". Finally, the technical solution should not create legal risks in the regulatory system (compliance) (BIS, 2017,p. 16): "DLT can increase risks if there is ambiguity or lack of certainty about an arrangement's legal basis. Because the application of this technology to payment, clearing and settlement activity is new, the legal underpinning for certain activities may not be as well established as that for traditional systems [...].".

Based on the highlighted statements, we can model the following set of functional and non-functional engineering requirements that define our problem:

1. Transparency: all market participants must be able to read the ledger.

2. Allowlist/blocklist: only those allowed by the regulator must be able to be an investor.

3. Issuers responsibility: issuers must be responsible for their tokens (tokenized assets) throughout their life cycle, from creation to destruction.

4. Regulation oversight: regulators must be able to know who the parties engaged in all market transactions are.

5. Regulation enforcement: regulators must be able to force or forbid transfers of assets — i.e., move assets on the ledger — to fulfill their duties.

6. Extensibility: the technical solution must be able to evolve along with the regulation.

7. Compliance: the technical solution must not create legal risks for the regulatory system.

8. Assets recovering: investors must be able to recover their assets in case they lose access to their private keys.

3 Problem: Implementing Financial Regulation Over a DLT

In this section, we design the solution based on the engineering requirements we previously defined.

3.1 Addressing the transparency and regulation oversight requirements

The first requirement in our list states the need for transparency in our solution. As discussed in the previous section, transparency is relevant for market fairness, regulation oversight, investigation, surveillance etc. However, transparency is an intrinsic characteristic of DLTs. Thus, this is an already addressed requirement of our solution, and we also met the requirement of 'regulation oversight'. There is a relevant discussion about the right balance between transparency on one side and confidentiality and privacy on the other (de Vilaca Burgos *et al.*, 2017). This is, though, a discussion outside the scope of this paper. For our purposes here, any combination of regulation and technology to address this issue will not conflict with our solution here.

3.2 DeFi architecture as a starting point

An essential element of our design is to define where in the market architecture (built on DLT) we will arrange the financial regulation. Let us use the architecture of DeFi to understand our possibilities and as a starting point for the architecture we will define.

DeFi is a financial ecosystem built on DLT to disintermediate and decentralize legacy ecosystems by eliminating the need for some traditional financial intermediaries and centralized institutions (Auer *et al.*, 2023). The core technological element of DeFi is the smart contract. A smart contract is an agreement between two or more entities translated in the form of computer code that runs on a DLT (Tran (Tran *et al.*, 2022). We can use a four-layer architecture to understand the DeFi ecosystem (IOSCO, 2022, p. 3):

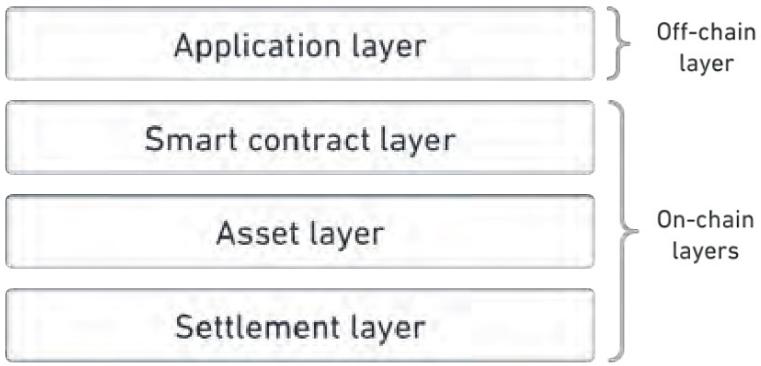
1. The settlement layer: DLT and layer 2 solutions where the consensus state of the DLT is maintained, i.e., transactions are recorded, and participants and smart contracts have addresses that can hold tokens and interact with other participants and smart contracts.

2. The asset layer: tokens that participants and smart contracts create and transfer on a DLT.

3. The smart contract layer: smart contracts provide functionality to DeFi products and services.

4. The application layer: front-end user interfaces, APIs, and other code that allow participants to interact with the smart contracts.

Figura 1 - Architecture of the DeFi ecosystem



In this architecture, there are three 'on-chain' layers — namely, (i) settlement; (ii) asset; and (iii) smart contract. In an on-chain layer, all data storage takes place in the ledger, and all computation — i.e., smart contracts execution — is made by the peers of the network. And there is one off-chain layer — (iv) application. An off-chain layer comprises the components that interact with the DLT. That said, we may now reflect upon the possibilities of arranging the financial regulation.

3.3 The need for adjudicators

The requirement of 'regulation enforcement' states that "regulators must be able to force or forbid transfers of assets — i.e., move assets on the ledger — to fulfill their duties." Also, the requirement of 'compliance' states that we must look for compliance with the current financial regulatory framework. This implies the need for adjudicators on the DLT to act on behalf of regulators. An adjudicator is a trusted third-party entity appointed by regulators to enforce compliance on the DLT. Moreover, to comply with the current legal system, regulators must be able to make ad hoc decisions and submit such decisions to be

executed by issuers together with adjudicators. Thus, we decide that adjudicators will be participants of the market along with issuers and investors (*e.g.*, OECD, 2020, p. 35). Note that, in practice, the role of an adjudicator on the market may be fulfilled by a government authority, a financial intermediary, or any other private entity accredited by regulators.

3.4 A regulation layer without smart contracts

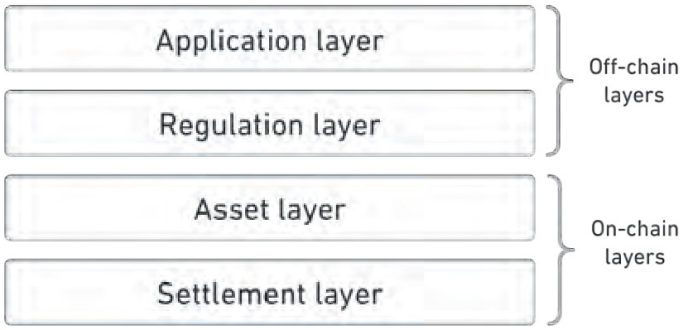
As we had seen previously, in the DeFi ecosystem, smart contracts encode all the rules that financial products and services are subject. *In our case here, since regulators always have the final word, it would not make sense to encode financial regulation into smart contracts because such smart contracts would always require some breach to enforce the decisions emanated ad hoc, which defeats the initial purpose of using smart contracts* (Wang; Chen, 2019, p. 197). This is precisely the argument that many scholars have raised in the situation where one tries to aggregate the current legal systems, regulators as participants on a DLT, and smart contracts:

> This problem may be evaded by allowing a general exception of 'force majeure', which may be invoked by the debtor, and is effectuated by calling an expert oracle. Thereby the contract enlists the aid of an outside expert or adjudicator. This in effect allowing Alternative Dispute Resolution (ADR) or Online Dispute Resolution (ODR) within the smart contract. The major disadvantage of this approach is that this effectively denies most of the benefits that smart contracts provide, namely, the automatic execution of the contract. (Tai, 2019, p. 92)

The only scenario in which encoding financial regulations into smart contracts would provide benefits is when the entire regulatory framework is automated as smart contracts. At this moment, with the complexity of the regulatory framework in any jurisdiction throughout the world, such an endeavor is virtually impracticable. Even though we disregard it, it would still be impracticable because it opposes how the legal system works.[1]

In short, the fact that regulators always have the final word, and make ad hoc decisions, drains out the possible benefits of encoding regulation into smart contracts. Thus, we decide that the financial regulation shall take place as an off-chain layer, as in the following figure:

Figura 2 - Architecture for a financial market with a regulation layer



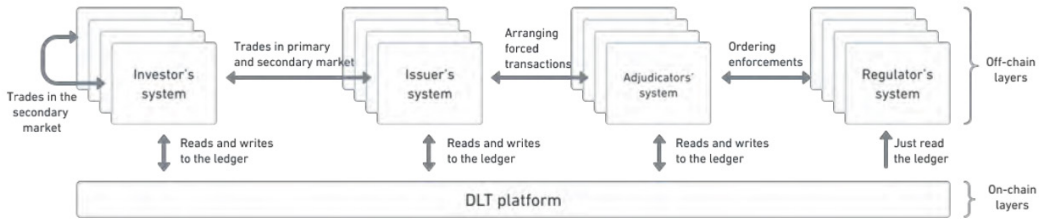
1 In the next section, we will delve deeper into this discussion.

This means that financial regulation will be implemented within the participants' systems and by the interaction among these systems in the same way as the electronic arrangements of financial markets do without DLTs. Now, we need to define a mechanism to connect the regulation layer with the on-chain layers of the architecture of our market built on DLT. We will create this mechanism in the following subsections.

3.5 Connecting the regulation layer with the on-chain layers

In our solution for a market (built on a DLT), there are three different roles: (i) investors; (ii) issuers; and (iii) adjudicators. These are almost the same market participants we previously defined, except for adjudicators. Adjudicators are participants that act on the DLT system on behalf of regulators. The following figure depicts the systems of each market participant, the off-chain interactions among participants, and the interactions among participants with the DLT platform. Each investor, issuer, adjudicator, and regulator have its own system:

Figure 3 – Systems of market participants



As we already discussed, regulatory processes occur on the off-chain regulation layer. Once a regulator needs to act on the ledger to enforce regulation compliance, it will send an order to the involved issuer and the adjudicator. Together, these two will send a new transaction to the ledger to perform the order. This new transaction will update the ledger to assure compliance with the regulation. In practice, this means transferring tokens from one wallet to another. Although a DLT protocol may comprise different kinds of transactions, the transaction that matters here is the most basic one: the transfer of tokens from one wallet to another. A solution where adjudicators act with issuers to create new transactions in the ledger as required is enough to assure the financial regulation of a secondary market in our DLT-based solution. We can do this using multi-signature wallets.

3.6 The core element: multi-signature wallets

Whereas in the DeFi architecture the smart contract is the core element, in our architecture, the core element is the multi-signature wallet. A wallet is the component of a DLT system that enables the management of funds by end users. From the point of view of DLT end users, a wallet is analogous to a bank account, where one stores funds and performs operations (Lipton; Treccani, 2021, p. 51). A multi-signature wallet is a wallet that requires multiple parties to operate the ledger. This is useful to implement what is called the 'four-eyes principle':

> In order to mitigate the risk of centralized trust, one often defines a transaction *approvalworkflow* such that multiple independent parties approve the operation. At a minimum, a four-eyes principle is enforced: a submitted operation must gather the validation of two users before its execution. By extension, more elaborate schemes may be defined, such as a so-called M by N multi-approval scheme where m parties must approve the operation out of a total of n potential approvers. This scheme generalizes the four-eyes principle to an M eyes principle and defines the total number of users authorized to participate in the quorum.Approval workflows may be implemented on-chain, i.e., directly on a distributed ledger, or off-chain, i.e., in a traditional service on top of a distributed ledger. (Lipton; Treccani, 2021, p. 287)

The four-eyes principle allows us to implement the due financial regulation right in the transactions submitted to the ledger. For simplicity's sake, we use a DLT that implements the four-eyes principle on-chain. Many DLTs implement on-chain *m n* multi-signature wallets — i.e., for a transaction from such wallet to be approved in the ledger, it must have at least *m* from the *n* possible signatures. A multi-signature wallet is generated by a set of *n* public keys. Each of the *n* possible signatures is generated by a private key associated with one of the *n* public keys. In the primary use case of multi-signature wallets, one wants that each of *n* independent entities has the power to add only one signature to a transaction. Thus, one creates a scheme where one needs the approval of *m* independent entities to submit a valid transaction into the ledger.

In our market scenario, all investor's wallets will be multi-signature wallets, where each of the market participants we previously defined — namely, issuers, investors, and adjudicators — have the power to add only one signature to a transaction. Issuer's wallet will be regular (not multi-signature) and used to issue any number of different custom tokens they create. For example, a financial institution, in the role of an issuer, may issue security tokens for multiple companies. In this scheme, an issuer can sell tokens in the primary market using only its own signature.

Investors' wallets will be (2 3) — i.e., it requires two of the three signatures to move the funds from their wallets. We will name them *A B* wallets. An *A B* wallet is a wallet that uniquely binds an investor *A*, an issuer *B*, and one adjudicator in this market. An investor *A* will have as many of such wallets as the number of different issuers among the tokens it holds. For example, suppose investor *A* holds in its portfolio some amounts of three different tokens *X, Y* , and *Z*. Tokens *X* and *Y* are issued by issuer *B*, whereas token *Z* is issued by issuer *C*. In this case, investor *A* will have two different wallets: wallet *A – B* and wallet *A – C*. In wallet *A – B*, it will hold its amounts of tokens *X* and *Y* ; in wallet *A – C*, it will hold its amount of tokens *Z*.

An *A B* wallet is generated using the investor public key, the token issuer public key, and the adjudicator public key. In this scheme, an investor cannot move tokens from its wallet alone. One can see an investor's wallet as a sort of 'account' it has with an issuer. Thus, an issuer can add signatures in transactions from any wallet that holds its issued tokens. Finally, the adjudicator has the power to add signatures in transactions from any *A–B* wallet within our market.

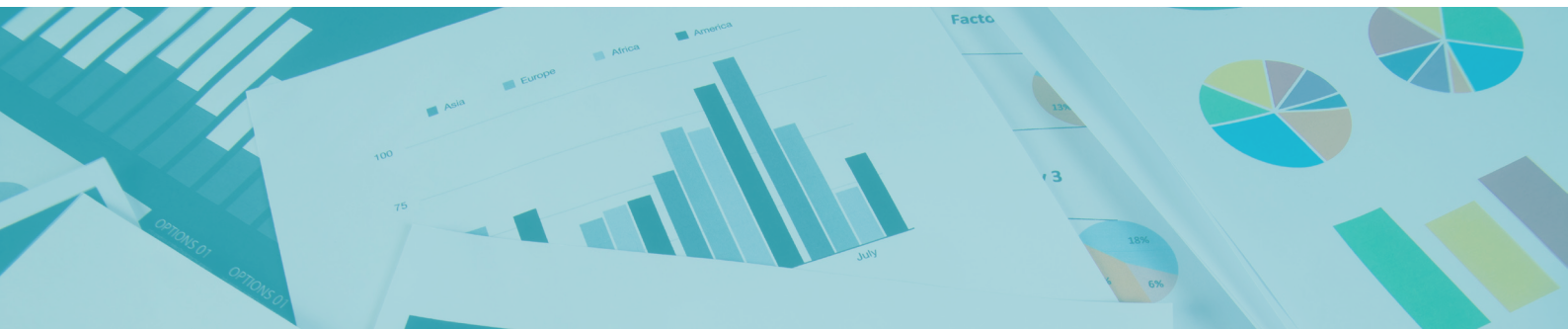


Figure 4 – Diagram of interactions among market participants

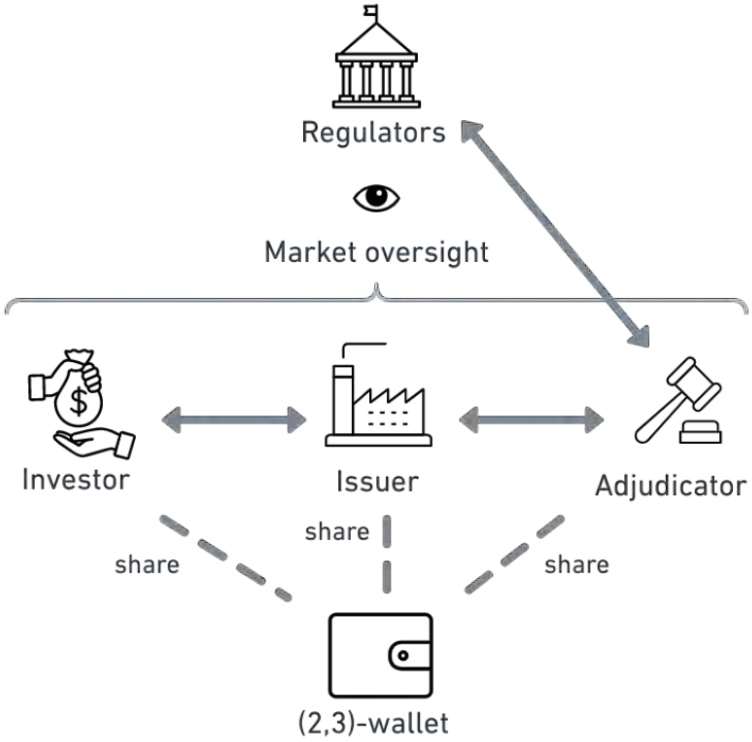


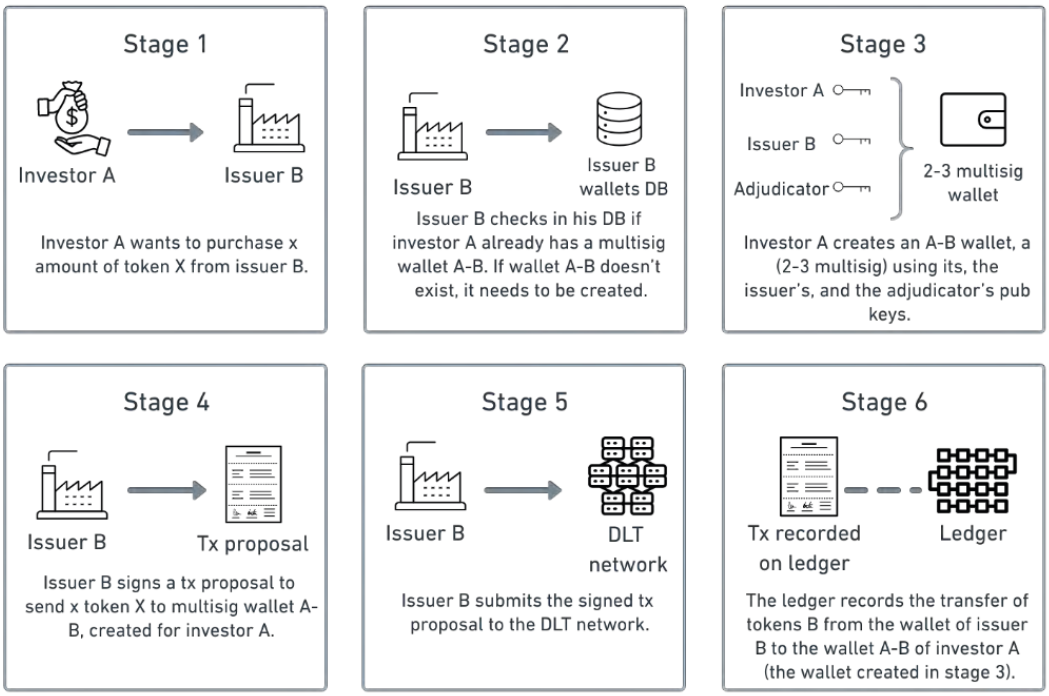
Figure 4 represents the interactions among the main market participants, using a multi-signature wallet as the core element. As we already explained, an investor's wallet is a (2, 3) wallet that binds an investor, an issuer, and an adjudicator. Each of these three has a 'share' in the wallet. No one alone can move the funds from the wallet. Despite being unable to move its funds by itself, the assets held by the investor's wallet are, in the eyes of regulators and the eyes of the law, indeed the investor's property.

Also, in Figure 4 we can see how market participants interact. Regulators oversee the whole market activities but only directly interact with adjudicators. They emanate orders to be enforced by adjudicators. To execute such orders, adjudicators interact with issuers. In addition to interacting with adjudicators, issuers also interact with investors in case of sales. In the following subsections, we will discuss how this arrangement allows our solution to meet all financial regulation requirements we had previously defined. For simplicity, we will suppose a market with a single adjudicator.

3.7 A sale in the primary market

Figure 5 is a storyboard explaining the process of selling tokens in the primary market:

Figure 5 – A sale in the primary market



The process we explain in this subsection does not belong to the secondary market but to the primary market. Despite this, it is paramount to address it to explain how our solution works and prove that it can also be applied to primary markets.

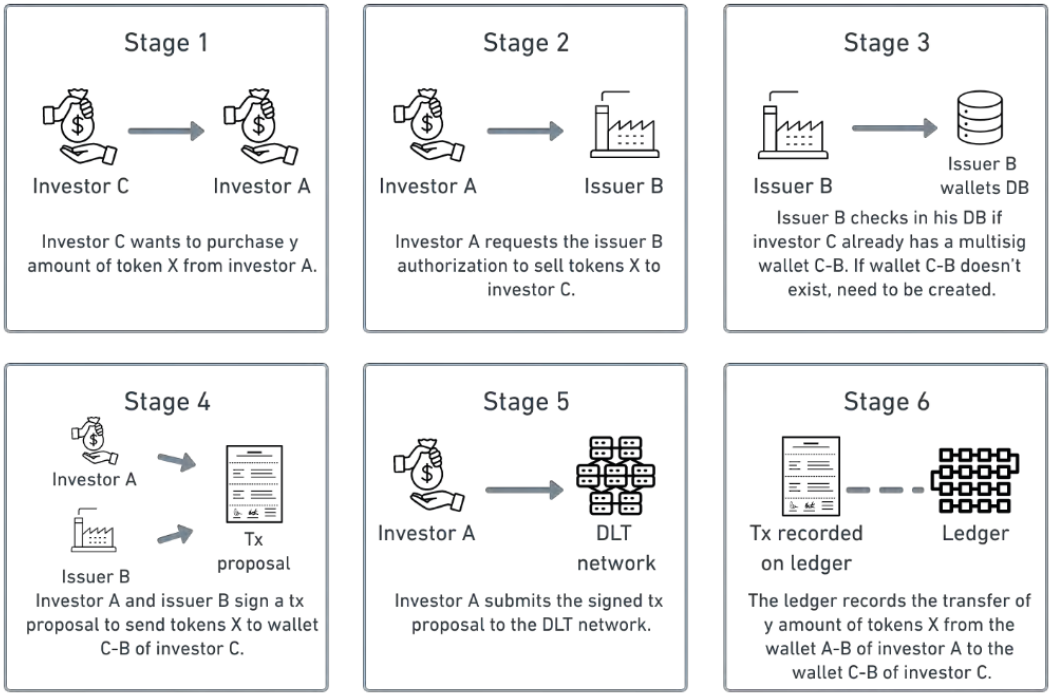
Note that what Figure 5 explains is the process of transferring tokens from issuer *B* (seller) to the investor *A* (buyer). However, this is just one side of the trade they are doing. The other side of the trade is the transfer of assets from the investor to the issuer. We are not depicting details of the whole trade because it is not necessary to explain our solution, but it is implicit that it is happening, regardless of the method of payment used.

In Figure 5, we see the process of issuer *B* selling x amount of token *X* to investor *A*. Stage 2 depicts issuer *B* checking in its database of token holders if investor *A* is or was a holder of any of its issued tokens. This meets the requirement of 'allowlist/blocklist'. Stage 3 depicts the creation of a new *A – B* wallet for investor *A*. This only happens if investor *A* does not hold and never held before tokens issued by *B*. Otherwise, even though the sale occurs in the primary market, investor *A* will use the *A – B* wallet it already has. With this, what remains in the three subsequent stages of Figure 5 is actually the basic life cycle of a DLT transaction.

3.8 A sale in the secondary market

Figure 6 is a storyboard explaining the process of selling tokens in the secondary market:

Figure 6 – A sale in the secondary market



In stage 1 of Figure 6, we see that two investors want to make a trade between them. Again, we are not depicting both sides of the trade for reasons already discussed. This trade is the basic operation that takes place in a secondary market. In stage 2 we see investor *A* requesting authorization to issuer *B* to sell its tokens *X*. This meets the requirement of 'issuer responsibility', which states that "issuers must be responsible for their tokens (tokenized assets) throughout all its life cycle, from creation to destruction." Issuer *B* will then see if investor *C* is a valid token-holder for tokens *X*. If investor *C* holds or has held tokens *X*, thus it already has a *C* B wallet. Otherwise, a new *C B* wallet needs to be created. This happens for the same reasons, and in the same manner, we see in the sale in the primary market.

It is helpful to cover the situation for markets in which investor *C* was once able to purchase tokens *X* but, for whatever reason, is not able anymore. In the example depicted in Figure 6, we consider investor *C* already has the *B C* wallet. Thus, it was already considered a valid investor for this specific asset (token *X*) by the adjudicator. Note that in the case of the primary market and here, we can increase the level or participation of the adjudicator without significant changes in our solution. For example, in the case of Figure 6, we could add a new stage after stage 3, in which issuer *B* requests the adjudicator to endorse the sale, even though investor *C* already is a token-holder of token *X*.

Remember that an investor's wallet is always a (2-3) wallet, where the three entities are the token's issuer, the investor that holds the tokens, and one adjudicator. In the case of a regular sale of the secondary market, both the investor selling its tokens and the token issuer needs to sign the transaction. With this, any attempt to move tokens to an unauthorized wallet is blocked by the issuer — using its allowlist/blocklist processes.

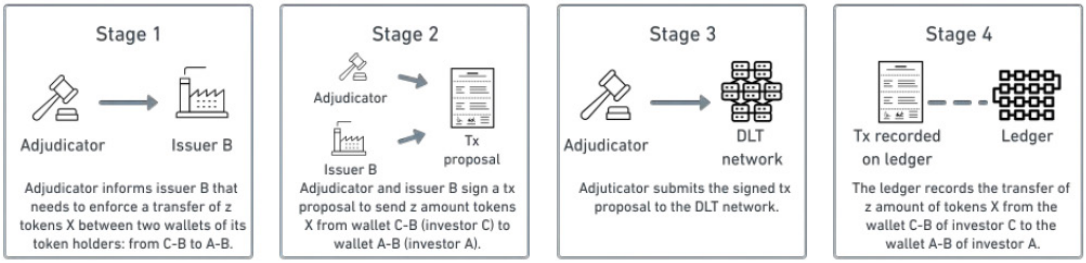
This is what we see in stage 4 of Figure 6. Once investor *A* collects the issuer's signature, it can proceed, relaying the transaction proposal to the DLT network. If all transaction data is valid, the transaction will be validated by the network peers (the DLT network nodes) and added to the ledger. Investor *A* has transferred some amount of tokens *X* from its wallet *A–B* to the wallet *C–B* of investor *C*. With this, we entirely met the 'issuers responsibility' requirement.

Moreover, we also entirely met the 'regulation oversight' requirement, which addresses 'regulation oversight': "regulators must be able to know whom are the parties engaged in all market transactions." In the arrangement we defined for selling in the primary and secondary, the adjudicator participates in the creation of all new wallets (providing its public key) that are used in the whole market (primary and secondary). This assures that it indeed has the resources to oversee market activities.

3.9 A forced transfer

Figure 7 is a storyboard explaining the process of a forced transfer taking place in the market:

Figure 7 – A forced transfer



Assets freeze and forced transfers are the two devices the adjudicator has on hand to enforce compliance in the market. With these two, together, we entirely meet the 'regulation enforcement' requirement. Figure 7 depicts the example that follows. First, take the example of the previous subsection (Figure 6), where investor *A* and investor *C* make a trade. Investor *A* transferred *y* amount of token *X* to investor *C*, and thus, it fulfills its part of the trade. We did not discuss the counterpart of this trade — i.e., what investor *C* agreed to provide to investor *A* —, but let us suppose investor *C* did not fulfill its whole part of the trade. Investor *A* thus appeals to the adjudicator. The adjudicator then processes the case and, as a result, decides that z amount of token *B* of the trade shall return to investor *A*. The adjudicator thus needs to perform a forced transfer.

Since investors' wallets are always 2 - 3, the adjudicator cannot make a forced transfer alone. It needs to pair with the issuer, which makes sense since it is responsible for its tokens throughout the whole token life cycle. The adjudicator informs issuer *B* that it needs to make a forced transfer. The adjudicator and issuer *B* sign the transfer. In stage 4, we see a transaction added to the ledger, recording a transfer of z amount of token *X* from wallet *C* – *B* (from investor *C*) to wallet *A* – *B* (from investor *A*).

3.10 Assets freeze

With the scheme we discussed until now, assets freeze by the adjudicator becomes a trivial operation. For example, if, for whatever reason, an investor in the market is under investigation, and its assets need to remain frozen, the adjudicator broadcasts a message to all issuers, stating that issuers should not sign transactions from (and maybe even to) this investor. If no new transactions can be done from investor wallets, in practice, all its assets are frozen. This is a broad case. In a narrower situation, the restriction may freeze only some of the wallets of the investor.

3.11 Assets recover

The last functional requirement we need to meet is 'assets recovering'. As we already discussed, each investor has a number of wallets equal to the number of different token issuers among the tokens it holds in its investment portfolio. Remember that these are all (2 3) wallets bound to the respective token issuers and the adjudicator. To manage this entire set of wallets, the investor just needs to use one private key. If the investor loses access to its private key, it can request help from the adjudicator. The adjudicator does not know and cannot recover the investor's old private key. Actually, nobody besides the own investor — and potentially its custodian agent — should know its private key.

What the adjudicator could do, is act alongside the issuer of the tokens stored in the wallet and create a transaction transferring the tokens from the old investor's wallet to a new one. The investor recovers access to its assets in this new wallet, whereas the old one becomes useless in practice.

3.12 Addressing non-functional requirements and other remarks

Throughout this section, we presented how the solution meets the functional requirements of the problem. It now remains for us to check whether the proposed solution meets the non-functional requirements. The solution maintains the entire financial regulatory framework, meeting the 'compliance' requirement. The solution allows for rapid evolution as changes occur in this same regulatory framework, thus meeting the requirement of 'extensibility'.

Finally, a remark about the use of adjudicators. For the sake of simplicity, we employ an example of a market with just one adjudicator. However, nothing prevents multiple of them from operating in the same market. In turn, regulators of a given market may centralize the role of adjudicator in a single government authority. Such arrangements do not change the format of investors' wallets: they remain linked to only one of these multiple adjudicators, and only this one has the power to enforce compliance in that wallet.

4 Discussion: Off-chain vis-à-vis on-chain financial regulation

When we talk about adding financial regulation into a market based on DLT, the principal design choice is whether to implement this on-chain or off-chain. In our solution, we chose to do it off-chain. One of the main reasons for this choice is that, in the given context, it is necessary to have adjudicators that have the final word, which drains out the advantages of financial regulation on-chain.

A possible mid-term solution would be the adoption of a hybrid regulation layer. In this alternative, one encodes the regulation into smart contracts as much as possible but still provides room for off-chain decisions. This is made by adding oracles in the smart contracts. Adjudicators would assume roles as oracles to fulfill the parts of the regulatory framework that, for whatever reason, could not (or is not desirable) be automated by a smart contract.

Although it is a possible solution, in the context described in this paper, the costs outpace the benefits and make it a suboptimal alternative. This is due to the following reasons: (i) lack of compliance of smart contracts with the current legal framework; (ii) high cost to develop smart contracts; (iii) high security risks of smart contracts; and (iv) low performance of smart contracts. In the remainder of this section, we will elaborate on each reason.

4.1 Lack of compliance of smart contracts with the current legal framework

A significant part of the regulatory framework occurs inside a given jurisdiction's judiciary system. Because of this, the compatibility of the technology in which one implements financial regulation with the legal framework is paramount. However, at the moment, there is still too much uncertainty in all jurisdictions throughout the world regarding the validity of smart contracts as binding contracts (OECD, 2020, p. 20) — i.e., legally enforceable agreements.

Notwithstanding, scholars are still debating if and how smart contracts that are defined ex ante might be compatible with the ex post nature of the judiciary system Borgogno (2019, p. 292). Because of these issues, using smart contracts inevitably brings legal risks that undermine a hybrid solution. In turn, such risks are bypassed using an off-chain regulation layer since it keeps the whole regulatory framework operative as is in the legacy system (Mills *et al.*, 2016, p. 29).

4.2 High cost to develop smart contracts

Smart contract development is the most expensive part of implementing a DLT solution in a given setting. In the labor market, the demand for engineers skilled enough to develop smart contracts outpaces the supply. This makes such professionals expensive and challenging to acquire. And such a scenario may not change soon because this happens not just due to the technology being new but also due to its level of complexity. Once deployed in the ledger, smart contracts are immutable, which makes it crucial that the code be free of bugs and security breaches. Beyond that, there is also the issue of being capable of translating the financial regulation parlance into code (BSI, 2019, p. 56) and the issue of the institutions that make up the regulatory system being able to audit such

contracts to assure compliance, which is another challenge and also add up with the costs (OECD, 2020, p. 20). For all these reasons, an on-chain solution would have a higher cost.

In turn, an off-chain solution benefits from the fact that it will not just use the regulatory framework itself but also part of the information systems implementing them. Also, even the new systems and components that market participants need to implement would require more easily obtained labor. Thus, the off-chain solution has a better cost-benefit than an on-chain solution.

4.3 High security risks of smart contracts

Bugs and security breaches in smart contracts have been a major issue of DLT technology for various reasons. First, because of how domain-specific languages used to code smart contracts are error-prone (BSI, 2019, p. 46). The error- prone issue of smart contracts is a problem that becomes bigger due to the scarcity of skilled-enough professionals to deal with the complexity we discussed in the previous subsection. *And this already bigger problem has a high impact due to the inherent immutability of smart contracts:*

> For smart contracts, the immutability of blocks implies that source code can no longer be modified once it is embedded into the blockchain. It is thus essential that the code be free of bugs. However, analysis has shown that a large part of existing smart contracts exhibits bugs, which are sometimes elementary. Some studies estimate their rate at about 45% of all Ethereum smart contracts. (BSI, 2019, p. 46)

Bugs and security breaches also occur in an off-chain environment. However, in this case, there are a number of possible containment measures that can be taken that simply do not exist in an on-chain environment. For example, if a bug or security breach is detected in an off-chain system, the system can simply be shut down as a measure to mitigate losses. The same cannot be done with a smart contract.

The solution that has been given to deal with this serious problem is to make smart contracts 'upgradable'. In this case, during development, clauses are left so that the smart contract can be corrected in the future if necessary. However, this undermines most of the benefits of employing smart contracts in our context, and such clauses may also be seen as loopholes.[2]

4.4 Low performance of smart contracts

A smart contract is computer code stored in a ledger that runs on the virtual machine of the DLT. The virtual machine of a DLT runs on top of its network of nodes. Running smart contracts is a challenge for any DLT platform. DLT platforms can scale well to process transactions, but currently have poor performance to process 2019, p. 211). This does

2 One example of this happened recently in the reverse Wormhole hack: https://news.coincu.com/169754-jump-crypto-attack-hacker- recover-stolen/ An upgradable smart contract was used, changing the owner of funds. This was done after an order from the court.

not result from the architecture of the distributed system of the DLT, but from the very limitation of the computational capacity of the hardware of current CPUs.

Each DLT network node needs to process all or a subset of smart contract transactions (i.e., execute the smart contract), creating DLT bottlenecks. This brings serious scalability issues. In the case at hand, it makes no sense to bear such a cost of poor performance.

4.5 Closure of the analysis

Finally, the off-chain regulation layer better meets our non-functional requirements: 'extensibility' and 'compliance'. In a moment where the world is still tailoring the harmony between DLTs and the legal system, we need a solution that makes it possible to evolve along with regulation. The immutability of smart contracts does not help with it. Also, as we discussed, with the off-chain regulation layer, the solution fully complies with the current regulatory framework. In contrast, with an on-chain layer, we increase legal risks and uncertainty.

As OECD (2020, p. 21) states: "moving from legacy infrastructure to DLT-based networks requires significant investment from market participants, and can only be expected to materialize once efficiency gains are proven and measurable for each asset type". Implementing financial market infrastructure based on DLT comes with a high cost, and as we stated right in the first sentence of this paper, the financial industry understands the potential and is willing to pay.

Now, from this, which we might call a starting point to the point where we have a good trade-off to implement financial regulation as an on-chain layer, there is a chasm. There is much uncertainty regarding the legal aspects of smart contracts, there is a long way to improve the security of smart contracts (Pise; Patil, 2022, p. 13), the computational cost is high, and last, moving from legacy infrastructure to DLT is a major endeavor that needs to be smooth. Regarding the challenges to adoption and implementation Mills *et al.* (2016) states:

> The legal framework (for example, statutes, regulations, policy, and supervision) governing financial markets and the conduct of PCS activities is well-established. Much of the existing legal environment, however, is organized and implemented in a manner consistent with the current financial market architecture, which has a complex network of participants that perform various functions and are regulated, supervised, and overseen by a diverse group of regulators. The relevant laws, regulations, and supervisory policies are aimed at achieving broad objectives such as

> market transparency, safety and soundness of financial institutions, and the efficient and effective functioning of the broader financial system and are not generally intended to favor a particular electronic technology. (Mills et *al.*, 2016, p. 27)

Thus, we conclude that, at the moment, the better alternative to implement financial regulation into a secondary market is using an off-chain regulation layer as the solution we proposed. It allows the compliance of the solution with the current financial regulatory framework, avoids legal risks, and makes possible a smooth yet progressive movement to implement DLT into the financial market infrastructure.

5 Discussion: Choosing a DLT Platform

Making sure one can implement a financial regulatory framework is relevant when choosing a DLT platform. Because of this, in this section, we discuss the implications of our solution regarding the choice of a DLT platform.

5.1 Making the solution DLT-agnostic

The proposed solution is based on the premise that the DLT platform has two features: (i) creation of custom tokens (either as a native feature or using smart contracts); (ii) multi-signature wallets. Nevertheless, with a few changes, it is possible to make the solution applicable to any DLT platform. To make the solution DLT-agnostic, we just need to use two technologies: (i) multi-party computation (MPC); and (ii) colored coins. With MPC, one moves the use of the four-eye principle off-chain. Thus, one can replace the use of a multi-signature wallet with MPC (Townsend; Zhang, 2023,p. 2). With colored coins, one can create custom fungible tokens into a DLT without using smart contracts or custom tokens creation (Lipton; Treccani, 2021, p. 75). Since these technologies are out of the scope of this paper, we will not explain how they work.

5.2 Implementing the solution using Hathor as the DLT platform

Despite the proposed solution being agnostic, this does not mean there is no difference in effectiveness, efficiency, and cost-effectiveness in deploying and operating it on different DLT platforms. That is far from the truth. A few crucial aspects need to be taken into account in the quest for the optimal technological trade-off to implement the best solution to a given context. We will discuss some of these aspects and argue how Hathor places itself as a good alternative of DLT platform in the context we discussed throughout this paper.

Note that we claimed that the proposed solution does not use smart contracts, which is true for the regulation layer. However, in most DLT platforms, smart contracts are still required to accomplish two critical functions of the financial market infrastructure: (i) create custom tokens; and (ii) make trades with atomic swaps. This is not the case with Hathor. The proposed solution is not just fully compatible with Hathor, but it is possible to implement it without using any smart contract in the financial market infrastructure.

Unlike most DLTs, in Hathor, there is no need to use a smart contract just to create a custom token. Custom tokens are created natively within the platform. The same happens

with atomic swaps. Atomic swap is a feature of DLTs that enables trades in a trustless manner. With atomic swaps, two parties can exchange their assets without needing to trust in each other or the assistance of a mutually-trusted third party, commonly known as escrow. In an atomic swap, transfers of assets from different participants are bound together in such a manner that either all transfers happen or none. On most DLTs, atomic swap is implemented via smart contracts, whereas on Hathor, it is a built-in feature, and is performed using a single blockchain transaction.

With this, the cost, time, and complexity of implementing a financial market infrastructure on Hathor become way lower than other alternatives while at the same time increasing the level of security and robustness.[3]

6 Conclusion

6.1 Reviewing the work

In this paper, we proposed a solution to implement financial regulation into secondary markets based on DLT. We first studied the principles of financial regulatory frameworks, and from this, we defined a set of requirements for our solution. After, we designed a solution based on these requirements. This brought us a solution for implementing financial regulation as an off-chain layer in a DLT-based financial markets framework. After that, we discussed why practitioners should use an off-chain layer rather than implementing financial regulation on-chain. Finally, we discussed how the solution stands in the face of the choice for a DLT platform. To wrap up this paper, we will present some final thoughts and list the key takeaways of this work.

6.2 Key takeaways

In the context where regulators always have the final word, it is not worth the cost to encode financial regulation into smart contracts. Furthermore, in the context we are dealing with, involving adjudicators and aiming to maintain compliance with the current regulatory framework, the best alternative is to implement financial regulation as an off-chain layer. Nonetheless, the solution retains the primary benefits of using DLT for PCS while circumventing the incompatibilities of smart contracts with the current legal system.

The key design element of the solution is to define a scheme of signatures suitable for the financial regulation, and thus all transactions added to the ledger are already compliant. This simplicity makes the solution a good alternative for transitioning the financial market infrastructure from legacy systems to a DLT platform. Finally, with Hathor platform is possible to implement a primary and secondary market of tokenized assets, as described in the solution, without using smart contracts, which makes it possible to obtain an optimal solution for this context by a reduced cost, risk, and time, and also bringing interoperability with the legacy systems and with the current regulatory framework. The

3 Explaining how it raises the security and robustness of Hathor platform is out of the scope of this paper.

conjunction of these factors implies more agility for entities to implement DLT-based solutions.

6.3 Work limitations

We decided to limit the scope of our work to the secondary market of tokenized assets to focus on the technical challenges of implementing financial regulation over a DLT. Extending the solution to the primary market is feasible using the same technical structure. It is only necessary to consider the whole life cycle of the assets and market participants — *e.g.*, onboarding of issuers, onboarding of investors, creation of tokens, destruction of tokens etc.

There are proposals to implement financial regulation in the settlement layer (Poncibò; DiMatteo, 2019, p. 122). In a nutshell, an adjudicator would be able to act directly with nodes that compose the DLT network or even revoke transactions already registered in the ledger. We did not consider this hypothesis because it either interferes with consensus or, even worse, removes the immutability of the ledger. Whatever the case, it weakens and potentially drains the benefits of using a DLT for PCS.

For the sake of simplicity, we presented the most relevant cases in the design of the solution, such as a sale in the primary market, a sale in the secondary market, a forced transfer etc. Despite this, our designed structure allows for addressing all edge cases that may arise, including adopting different alternatives for specific cases of different markets or jurisdictions.

References

ÁRVAI, Z.; HEENAN, G. A framework for developing secondary markets for government securities. **International Monetary Fund (IMF) Working Paper**, v. 08, n. 174, 2008.

AUER, R.; HASLHOFER, B.; KITZLER, S.; SAGGESE, P.; VICTOR, F. The technology of decentralized finance (defi). **Bank for International Settlements Working Papers**, n. 1066, Jan. 2023. [Online]. Available in: https://www.bis.org/publ/work1066.pdf

BANK FOR INTERNATIONAL SETTLEMENTS – BIS. International Organization of Securities Commissions. **Principles for financial market infrastructure and International Organization of Securities Commissions**. 2012. [Online]. Available in: https://www.bis.org/cpmi/publ/ d101a.pdf

BANK FOR INTERNATIONAL SETTLEMENTS – BIS. **Distributed ledger technology in payment, clearing and settlement: An analytical framework**. 2017. [Online]. Available in: https://www.bis.org/cpmi/publ/d157.pdf

BORGOGNO, O. Usefulness and Dangers of Smart Contracts in Consumer Transactions. In: DIMATTEO, L. A.; CANNARSA, M.; PONCIBÓ, C. (ed.). **The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms**. Cambridge, UK: Cambridge University Press, 2019. p. 288–310.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMMATINSTECHNIK – BSI. **Towards secure blockchains:** Concepts, requirements, assessments. 2019. [Online]. Available: https://www.bsi.bund.de/ SharedDocs/Downloads/EN/BSI/Crypto/Secure_Blockchain.html

FABOZZI, F. J. **Finance:** Capital Markets, Financial Management, and Investment Management. New Jersey, USA: Wiley, 2009.

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS – IOSCO. **Objectives and principles of securities regulation**. OICV-IOSCO, 2003. [Online]. Available in: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD154.pdf

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS – IOSCO. Descentralized finance report. **International Organization of Securities Commissions**, 2022. [Online]. Available in: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf

LIPTON, A.; TRECCANI, A. **Blockchain and Distributed Ledgers Mathematics, Technology, and Economics**. Switzerland: World Scientific Publishing Co Pte Ltd, 2021.

MAKAROV, I.; SCHOAR, A. Cryptocurrencies and decentralized finance. **Bank for International Settlements Working Papers**, n. 1061, Dec. 2022. [Online]. Available in: https://www.bis.org/publ/work1061.pdf

MILLS, D. et al. Distributed ledger technology in payments, clearing, and settlement. **Board of Governors of the Federal Reserve System: Finance and Economics Discussion Series**, n. 095, p. 3, Dec 2016. [Online]. Available in: https://doi.org/10.17016/FEDS.2016.095

MOMTAZ, P. P. Security tokens. **SSRN Electronic Journal**, 2021. [Online]. Available in: https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=3865233

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT – OECD. Policy framework for effective and efficient financial regulation: General guidance and high-level checklist. **OECD Blockchain Policy Series**, 2010. [Online]. Available in: https://www.oecd.org/finance/financial-markets/44362818.pdf

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT – OECD. The tokenisation of assets and potential implications for financial markets. **OECD Blockchain Policy Series**, 2020. [Online]. Available in: https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT – OECD. Regulatory approaches to the tokenisation of assets.**OECD Blockchain Policy Series**, 2021. [Online]. Available in: www.oecd.org/finance/ Regulatory-Approaches-to-the-Tokenisation-of-Assets.htm

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT – OECD. Why decentralised finance (defi) matters and the policy mplications. **OECD Blockchain Policy Series**, 2022. [Online]. Available in: https://www.oecd.org/finance/Financial-Market-Developments-and-Conditions-in-Asia.htm

PISE, R.; PATIL, S. A survey on smart contract vulnerabilities and safeguards in blockchain. **International Journal of Intelligent Systems and Applications in Engineering**, v. 10, n. 3S, p. 01–16, 2022. [Online]. Available: https://ijisae.org/index.php/IJISAE/article/view/2405

PONCIBÒ, C.; DIMATTEO, L. A. Smart Contracts: Contractual and Noncontractual Remedies. In: DIMATTEO, L. A.; CANNARSA, M.; PONCIBÓ, C. (ed.). **The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms**. Cambridge, UK: Cambridge University Press, 2019. p. 118–140.

VILACA BURGOS, A. de; OLIVEIRA FILHO, J. D. de; SUARES, M. V. C.; ALMEIDA, R. S. de. **Distributed ledger technical research in central bank of Brazil**. Brasília: BCB, 2017.

TAI, E. T. T. Challenges of Smart Contracts: Implementing Excuses. In: DIMATTEO, L. A.; CANNARSA, M.; PONCIBÓ, C. (ed.). **The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms**. Cambridge, UK: Cambridge University Press, 2019. p. 80–101.

TOWNSEND, R.; ZHANG, N. Technologies that replace a “central planner”. **MIT Economics Papers and Proceedings**, n. 204, 2023. [Online]. Available in: https://economics.mit.edu/sites/default/files/2023-01/InnovativeFinancialDesign_ AEAP_ PZhang.pdf

TRAN, D. A.; THAI, M. T.; KRISHNAMACHARI, B. **Handbook on Blockchain**. Switzerland: Springer International Publishing AG, 2022.

WANG, J.; CHEN, L. Regulating Smart Contracts and Digital Platforms: A Chinese Perspective. In: DIMATTEO, L. A.; CANNARSA, M.; PONCIBÓ, C. (ed.). **The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms**. Cambridge, UK: Cambridge University Press, 2019. p. 183–209.

ZETZSCHE, D. A.; ANKER-SØRENSEN, L.; PASSADOR, M. L.; WEHRLI, A. Dlt-based enhancement of cross-border payment efficiency – a legal and regulatory perspective. **BIS Working Paper**, n. 1015, May 2022.