Volksbanken Raiffeisenbanken
Cooperative Financial Network

Smart Bond Contract (SBC)

Towards a functional Redesign of a digital Security's Lifecycle

DZ BANK

Content

1. Introduction

Distributed Ledger Technology (DLT) has the potential to disruptively improve cross-company value chains in the financial industry. By contrast, from today's perspective, the wholesale fixed-income market is still largely characterized by manual, historically developed business workflows and fragmented technological system landscapes.

Most recently prominent issuers such as the European Investment Bank (EIB), KfW and Siemens took a pioneering role in the digitalization of bond issuances. In the course of the ECB Explorative Phase (ECB trials) digital solutions were explored to conduct settlement of DLT-based financial transactions against central bank money, for example via the Interoperability Mechanism provided by the Bundesbank. As a result of these trials the Eurosystem has decided to work on a productive digital settlement solution for DLT-based transactions. In addition to that, the BIS Innovation Hub and the New York Fed's New York Innovation Center published a study on the implementation of central bank policies in a tokenized world [1].

The mentioned projects as well as others have demonstrated the potential of digitalization along parts of the value chain of an issuance (e.g. settlement) and proved feasible. In its publication [2] on the state of a DLT-based capital market, KfW states based on its first two DLT-based securities issuances in 2024 that, in addition to "great opportunities for the European and international financial market", the technologies can also contribute to "processing financial market transactions more efficiently and securely".

The next logical step is to integrate the proven basic components into a **comprehensive functional framework** across the entire value chain. Rather than simply digitizing existing process chains, it is important **to rethink and redesign them**. The early establishment of accepted and transparent digital standards remains an essential necessity. Open collaborative partnerships can contribute significantly to the development of those standardized protocols and thus help to prevent the rise of new technical risks due to digital fragmentation.

In this publication we present the **Smart Bond Contract (SBC),** which digitally and functionally maps the lifecycle of DLT-based securities along the entire value chain from issuance to repayment. The concept aims to replace processes that have evolved over time and are fraught with friction and risk. Its aim is therefore to concretely contribute to the establishment of a functional protocol standard.[1]

2. Fixed Income Markets from the Perspective of Digitalization

Issuance processes are based on market infrastructures that have grown over time. This has resulted in cross-company interaction workflows that are only partially harmonized and non-standardized. Significantly delayed settlement periods result from media disruptions, a high level of manual effort, and time-consuming coordination procedures. There is a high need for digital standardization and ideally automation along the entire value chain.

The introduction of electronic securities through the Electronic Securities Act (eWpG) in Germany in 2021 established a legal basis for the digitalization of securities. This framework enables us to move beyond the current discussion of tokenization. The result is the rise of new standardized, functional business workflow designs that comply with applicable regulatory and legal requirements.

If properly designed, process efficiency can be significantly increased while operational risk is reduced. One of the most valuable objectives will be to reduce settlement times to T+0 (where T is the pricing day) and to achieve high-frequent settlement finality.

[1] The following concept focuses on the German Electronic Securities Act (eWpG) whereas it is also applicable to other jurisdictions

3. Potential of Distributed Ledger Technology (DLT)

The following section describes the fundamentals of Distributed Ledger Technology (DLT). It focuses particularly on the concept of Smart Contracts as distributed computer programs and their potential in the financial industry. In the realm of Distributed Ledger Technology we encounter decentralization in multiple aspects:

- Distributed data storage and management of digital claims (tokenization),
- Distributed program execution (Smart Contracts), and
- Organizationally distributed development of common standards and open software.

In contrast to conventional financial systems, which are usually maintained by market infrastructure providers, a DLT-based infrastructure enables digital interaction between market participants directly. **Digital disintermediation** enables distributed computer programs to partially take over classical service roles. Therefore, the technology has the potential to create new functional-driven ecosystems including innovative, modularized and digital service-chains. However, the financial industry has often interpreted DLT in form of new digital platforms and hence has not fully exploited its full potential on a large scale.

3.1 Distributed Software Operation

A classic computer consists of memory and a central processing unit (CPU), whereby data and programs (software) as deterministic instruction chains are managed in the memory and executed by the CPU once the program functionality is called. Since the emergence of the Internet, the distribution and execution of software have been largely centralized – a server is hosting the software which gets consumed by a so-called client computer. The Ethereum Blockchain introduced in 2015 establishes a Turing-complete[2] distributed computing engine. The "Ethereum Virtual Machine" (EVM) enables the synchronization of distributed operations across a network of computer nodes. Calling a function on one of these nodes results in a change to the memory state, which is distributed uniformly throughout the network after positive consensus. This decentralized approach to software operation may have a disruptive effect on the classic "client-server" mechanism. Ideally, the need for a central operator of software would no longer exist, and network participants would be able to install and access software functionality on an equal footing.

3.2 Smart Contracts

The term 'Smart Contract' has become established related to computer programs that are installed on a DLT-based infrastructure. Contrary to their name these programs are neither smart nor self-executing but rather deterministic command sequences. A special feature is that a Smart Contract can autonomously check which wallet address is invoking the provided functionality. The most native and currently most prominent use case related to Smart Contracts is **tokenization** - DLT-based management of digital claims. Token contracts such as the ERC-20 standard [3] have their own digital account management. The storage scheme is very simple: Balances are assigned to addresses based on a functional dictionary pattern. The functionality offered in the contract enables direct transfers between authorized participants dependent on predefined rules (e. g. sufficient balance). There is also another feature: Smart Contracts can act as **virtual escrows** if tokens are transferred to their address and thus are able to be processed algorithmically. This feature is particularly useful for processing **Delivery versus Payment,** i.e. the exchange of digital claims for digital payments using Smart Contracts in an atomic and functional way. One prominent example is the Hashed Timelock Contract (HTLC) mechanism[3]. This protocol has prominently been explored in the context of Bundesbank's **Interoperability Mechanism** with the aim to functionally connect DLT-based transfers with the existing T2 Settlement System.

3.3 Beyond Tokenization

Current use cases of DLT in traditional financial industry can be divided into three categories: Digital claims, such as those of a security, can be managed and stored

[2] Turing completeness of a computer system describes its universal programmability
[3] A Hash-linked Swap is a Smart Contract-based mechanism in which a secret key is used to functionally coordinate the transfer of digital claims across separated infrastructures. For example, locked cash tokens can only be claimed if an associated secret key is decrypted and published, which in turn can then be used by the opposite party to claim the security tokens residing on the other infrastructure.

digitally on a distributed database - these are referred to as **tokenized assets.** In addition to the digitization of paper-based processes, it can be said that tokenization does not add much value in itself. As a second category, central banks are working on functional solutions which link the transfer of tokenized assets with digital forms of central bank money (wCBDC[4]) - ideally a tokenized solution will be introduced in the future. These two basic building blocks pave the way for the third category which are so-called **Smart Financial Contracts (SFC).**

The potential of such "smart" financial product designs lies in utilizing the described advantages of DLT-based Smart Contracts. A Smart Financial Contract can authorize the invocation of certain functionality based on predefined process states, execute them deterministically and is also able to publish events to the main event queue which enables the design of automatable Event-Driven Workflows. A concrete example of such a product and process innovation is the Smart Derivative Contract **(SDC).** The aim of this product is to completely redesign the post-trade process of a bilateral OTC derivative while eliminating existing contractual risks and process frictions. With features such as automatic termination and a payout profile based on a prefunding mechanism the concept represents a structured financial product and motivates a business case by eliminating counterparty credit risk.

3.4 Open Digital Standards

In addition, distributed, open-source driven software development can play a key role in a bottom-up driven development of digital **financial standards.** The largely anonymous Ethereum community has introduced the so-called "Ethereum Request for Comments" (ERC)" process for the submission of Smart Contract-based standards. The ERC-20 proposal introduced in 2015 has become the first recognized standard for tokenization also in the regulated financial industry. An extended token standard is the ERC-3643, which regulates the lifecycle of tokens in compliance with regulatory requirements. The above mentioned Smart Derivative Contract was also published as a standard proposal: ERC-6123. We are convinced that this type of cooperative organization is crucial for creating win-win situations for market participants, as well as for developing and establishing secure and widely accepted digital standard protocols.

3.5 Guardian Fixed Income Framework

In November 2024 the Monetary Authority of Singapore (MAS) published the Guardian Fixed Income Framework (GFIF) [4] to foster the **standardization of DLT-based tokenized fixed income instruments** with the aim to increase acceptance among market participants. General guidelines and best practices for standardization are outlined. The use of the ICMA Bond Data Taxonomy as a digital data standard is recommended.

The publication points out that DLT offers considerable advantages with regard to the entire life cycle of fixed-income-based financial instruments. Smart contract-based procedures can be used to coordinate and standardize multi-party workflows in the primary market. Mechanisms such as algorithmic token transfers help to automate the workflows for settlement, maturity and repayment thereby increasing operational efficiency and reducing settlement risks. The technology also offers audit compliance thanks to the traceability of the transaction history. Depending on the selected DLT infrastructure, it is important to decide which data can be made public, and which should only be made selectively accessible. Transparent and configurable source code as well as an understandable and modular software design make a significant contribution to increase acceptance and usage. Existing regulated processes and productive system infrastructures must be kept in mind in order to ensure the best possible and minimally invasive integration.

4. Concept of the Smart Bond Contract

We specify these recommendations and introduce the notion of a **Smart Bond Contract (SBC)**. In alignment with the GFIF guidelines, the SBC is to be understood as a functional protocol which, in conjunction with a digital data format to functionally define the complete lifecycle of a digital security from issuance to redemption.

[4] wholesale Central Bank Digital Currency

4.1 Characteristics

The SBC protocol is designed platform-agnostic, an EVM-based implementation making use of above mentioned features of Smart Contracts is preferred to enable direct digital interaction between the acting parties. The Smart Contract can store and process data, taking over and orchestrating interactions in a rule-based manner. In analogy to the above mentioned Smart Derivative Contract, the Smart Bond Contract focuses on the execution of deterministic functionality throughout the entire lifecycle of a security via precisely defined process states. It consists of a standardized **data format** based on the ICMA Bond Data Taxonomy in combination with a **functional protocol.** The SBC approach aims to be a generic and modular concept that goes beyond simple entitlement management and token transfer.

4.2 Optimization of the Issuance Process

By using the SBC for a digital security the involved parties agree to use the above mentioned functional **interaction pattern** and a digital **data format** which offers a standardized and auditable single source of truth to which existing downstream systems can be linked. The predefined deterministic interaction mechanism aims to reduce time-consuming manual reconciliations and thus enable significantly shorter issue times.The advantages can be categorized as follows:

- **Streamlined processes:** By using the functionality, services provided by traditional intermediaries (such as the Initial Paying Agent [IPA]) can be digitized, which eliminates friction-laden cross-company process chains.
- **Increased efficiency:** Digitized issuance documents (term sheets, terms and conditions, etc.) stored directly in the smart contract creating a standardized data source for various stakeholders and systems.
- **Reduction of settlement risks:** Secure and automatable Delivery versus Payment on an intraday basis, which does not require centralistic transaction coordinators but rather lightweight oracle services (can increase settlement frequency and allow algorithmic intraday-funding (For the DvP protocol used see section 5.3)).
- **Management of intraday risks:** The aforementioned efficiency gains allow banks to better manage their intraday risks, which are moving further into the focus of supervision [5] .

5. Implementation Aspects

The aim of the SBC is to provide a configurable package of functions to implement the lifecycle of various securities and issuance types across different jurisdictions. The functional specification (interface) is designed to be platform-independent, whereby an EVM-compatible implementation and operation on a DLT infrastructure enabling the realization of the advantages mentioned in Chapter 3.

5.1 Core Modules

The SBC protocol is based on the XML-based ICMA Bond Data Taxonomy which serves as a uniform data source for recording security-related data and which get finalized based on predefined rules. The object-oriented functional design enables functional modules to be combined in a flexible way depending on the specific use case. The following smart contract "plugins" are proposed:

1. Process control via defined process states
2. Storage and processing of digital issue conditions & creating terms and conditions
3. Tokenization process and interaction with a regulated crypto registrar
4. Trade data confirmation (based on ERC-6123)
5. Automated Delivery versus Payment (based on ERC-7573)

Additional components can be added:

6. Roles and authorizations
7. Orderbook management

The execution of the functions provided is controlled autonomously by the Smart Contract based on predefined process states. The usage of the XSLT standard facilitates the automated creation of issuance terms and conditions by linking the contractual information to the security's data by using XSLT to connect the contractual context to XML-based parameters. As far as public availability is non-critical data records can be stored in the Smart Contract directly in an audit-proof manner and edited based on the Smart Contract's process states. The tokenization and settlement process uses efficient protocols such as ERC-7573 – described below. A functional interaction pattern for transaction data reconciliation can be implemented using functionality provided by ERC-6123, which uses a hash-based[5] mechanism to check whether both parties have agreed on the same transaction and trading data. Standardized event objects published by the Smart Contract to the DLT's event queue enable event-based and automated event-driven design.

5.2 Sequence Flow of a functional Issuance Process

The following sequence diagram shows a potential functional interaction flow for a Smart Contract-based issuance process (of a crypto security in terms of the eWpG), involving only one issuer and one investor. The interaction begins when the indicative terms of the issuance are uploaded in a specific Smart Contract registry. A registered investor can create a trade request which results in the installation of an SBC. The issuer then converts this request into a concrete trade offer, which the investor can confirm. Once the terms and conditions of the issuance have been finalized, the security tokens can be generated (a process known as

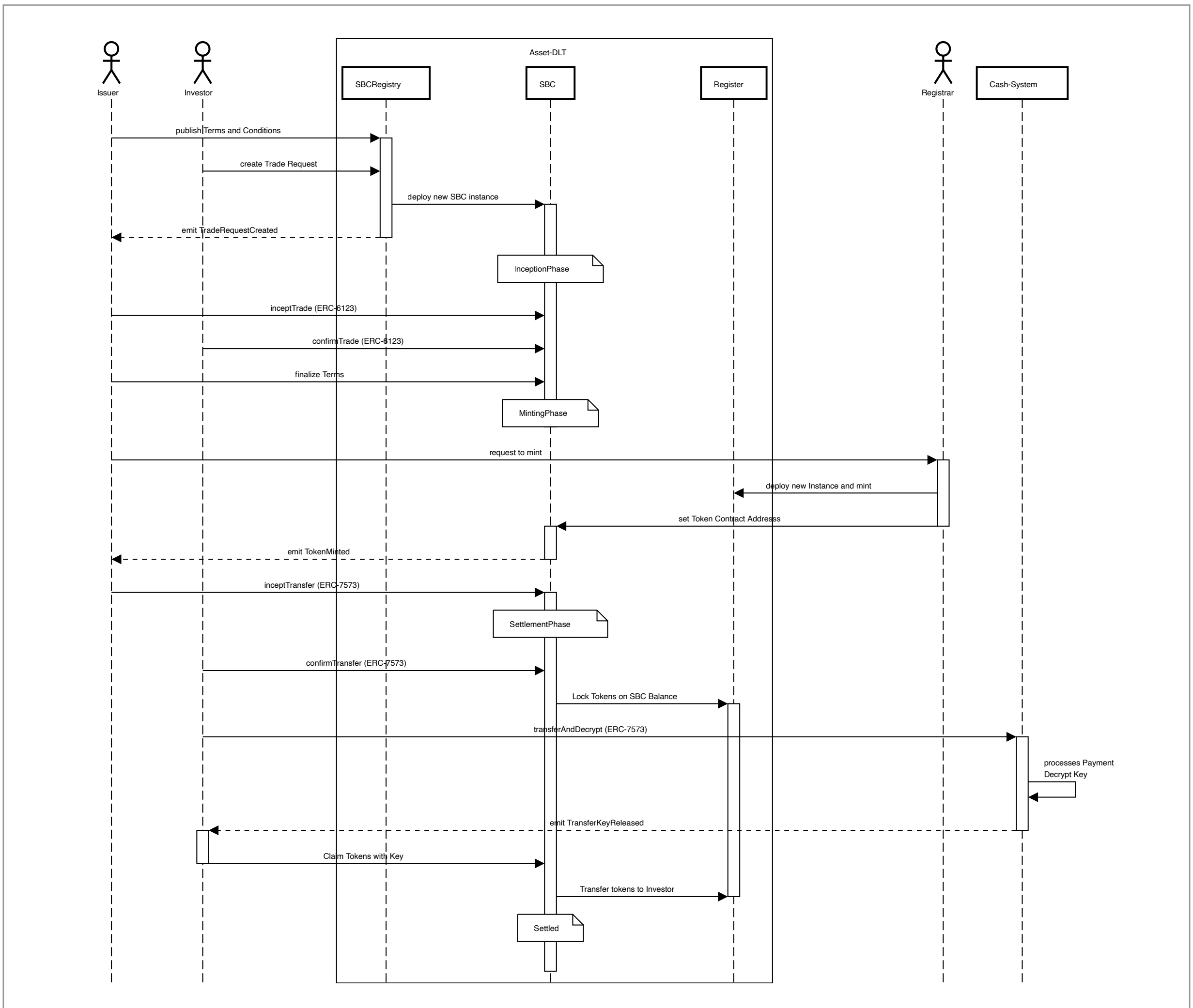


Figure 1: Sequence diagram of an issuance process with a smart bond contract
This diagram illustrates an idealized exemplary design for a functional issuing process. Depending on the infrastructure, settlement processing can mostly be conducted smart-contract based and automated. The trading and post-trading processes are clearly separated here. The DvP-interaction embedded in the above process follows [6].

[5] A hash function maps a dataset to a unqiue, fixed-length string of characters, commonly used to verify data integrity

minting), which involves the crypto registrar in a standardized and functional manner. Ideally, this interaction should occur on-chain or through provided off-chain APIs. Once the tokens have been generated, an automatable settlement protocol (based on ERC-7573,[4]) is followed. In this protocol the smart bond manages the tokens for the investor as a digital escrow until the payment has been processed and the respective key to claim the tokens has been released. The smart bond passes through various process states and shows the "settled" state at the end. The explicit definition of the process states is subject to configuration.

5.3 Decentralized Delivery versus Payment

The above functional design uses a Smart Contract-based Delivery versus Payment protocol, which can be used with separate asset and payment infrastructures. The ERC-7573 draft standard is favored, as it

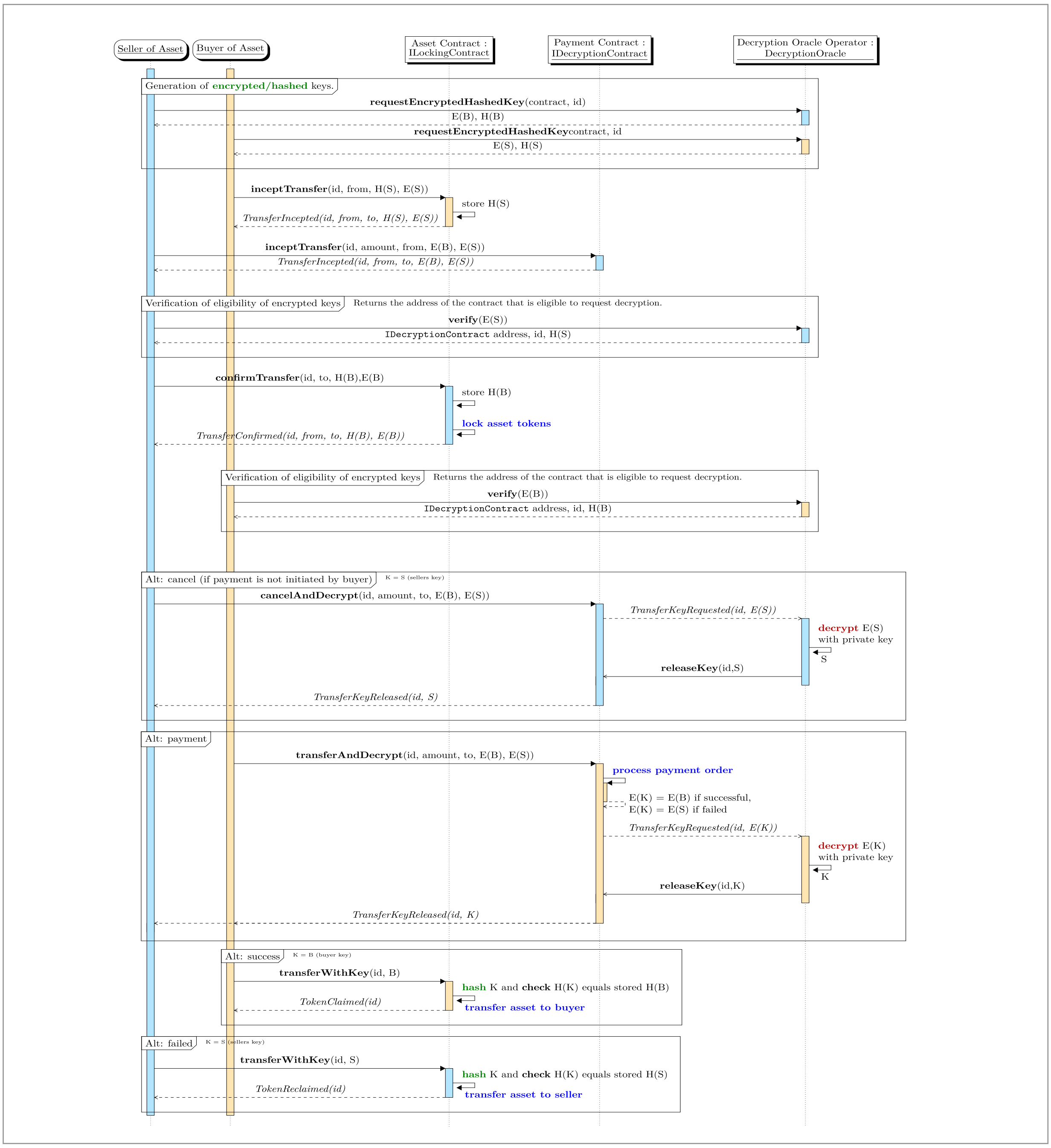


Figure 2: Sequence diagram of a stateless DvP

eliminates the known problems of the HTLC protocol, see [7] [8]. With HTLC protocols, a token is locked in a certain time-period. If no transaction takes place, it is returned after the time has expired. There may be a "race condition" in this procedure: Failure to collect the token in time, even though its payment was successful, for example because the necessary hash was received too late. The 7573-Protocol avoids the problematic time-lock mechanism. Token locking is only necessary on one infrastructure. A decryption process ensures that tokens without a time lock can only be retrieved by the authorized party.

This automatable method enables the decentralized and secure transfer of tokenized assets without the need for a central coordinator with knowledge of the transaction details. All that is required is an agnostic service ("Decryption Oracle"), which provides the decryption mechanism. Depending on the success of the payment processed on the separated payment infrastructure, this service publishes a secret key with which the asset tokens can be transferred to the authorized address. This service can be integrated on an event-based and automated basis. See Figure 2.

5.4 Interaction in Connection with a Custody Solution

The following diagram outlines how custodians, issuers and investors can interact with the SBC, depending on the wallet solution used.[6] Different constellations are possible, taking into account regulations regarding Digital Custody, while also enabling the involved parties to interact with each other by making use of the SBC's provided functionality. The interaction is separated in several parts. Accordingly, if a party has a wallet, they can access all the functions defined in the SBC by themselves and execute them in case they are entitled.

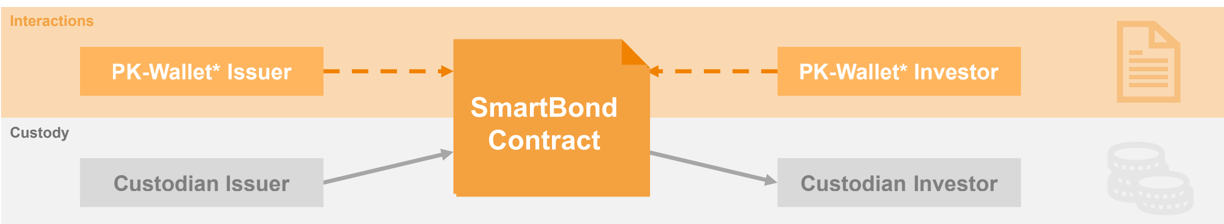
Separated wallets can be used for different tasks (indication, trading, settlement, custody, etc.). For example, dedicated wallets for investors and issuers would be used for calling specific SBC functionality – that is not subject to custody - while the custodian's wallet provides the address at which the tokens are managed in accordance with the crypto registrar. In this way, wallet-based interactions can be clearly separated from each other in accordance with regulatory requirements, while the entire workflow can still be conducted on one chosen infrastructure without media discontinuity.

6. Regulatory Aspects

As previously explained Smart Contracts are software programs stored on a DLT and executed on request by network participants. Therefore, they are the translation of what has been contractually agreed into machine-readable code[7]. Code-execution is designed to be deterministic and therefore predefined in advance, whereby the execution, i.e. the performance of certain actions or transactions, can be "halted" if the code allows for it.[8]

If these conditions represent events from the real world that are not already mapped in the DLT infrastructure on which the Smart Contract is typically based, these real-world events will have to be made available via interfaces to the real world - so-called "Oracles" - which supply the Smart Contract with external information[9].

The biggest advantage of blockchain Smart Contracts is that they are largely immutable and tamper-proof – properties that can fulfill proof (security) functions. Only if their code is immutable are Smart Contracts able to fulfill their main purpose – to promote trust in contractual fidelity. Finally, a DLT infrastructure is



*Private Key-Wallet

[6] A public-private key-based wallet is required for interaction on a selected DLT infrastructure. Using the private key, the respective entity signs a respective transaction, which is then validated in the network using the entity's public key.
[7] Leupold/Wiebe/Glossner IT-R/Kaulartz, 4th ed. 2021, Part 9.5 para. 18
[8] Ebers, Keyword Commentary Legal Tech, Smart Contracts para. 5
[9] Leupold/Wiebe/Glossner IT-R/Kaulartz, 4th ed. 2021, Part 9.5 para. 19

considered transparent, which makes the execution of Smart Contracts predictable.[10]

From a legal perspective, a Smart Contract must always be measured against the applicable law[11] which is a very dynamic matter in this respect given that German and European regulations are not yet fully aligned.

As the SBC is in general based on electronic securities in form of crypto register securities in accordance with the eWpG, we will briefly look at a few selected legal framework. The eWpG, the eWpRV (Regulation on Requirements for Electronic Securities Registers) and the DLT Pilot Regime (Regulation (EU) No. 2022/858) already provide the German market with a basic legal framework that can be used to issue, trade and settle electronic securities. However, a certain amount of practical experience still needs to be gained in some areas.

Regarding legal terms of contracts and their drafting, the main focus lies on the amendment of the bond terms and conditions to electronic securities (e. g. crypto securities), adjustments to the issuance and purchase agreements or the preparation of an information memorandum / securities prospectus. In many cases, however, traditional contracts can be used, which only need to be partially changed with regard to DLT-based securities.

Larger legal questions tend to arise in relation to the mapping of technical risks or legal issues in connection with wallets and the safekeeping of crypto securities and cryptographic keys,see also [2].

In addition further regulatory aspects need to be considered. For example, crypto securities within the meaning of the eWpG are not yet eligible for exchange trading, as the Central Securities Depository Regulation (CSDR) only permits multilateral trading in securities that are booked in the securities register and deposited with a central securities depository (Art. 3 (2) CSDR). Furthermore, crypto securities currently lack ECB eligibility as they are not yet recognized as "eligible collaterals".

Aligning such functional design proposals with existing regulatory frameworks is crucial. Therefore inviting regulators for an early review is desirable in order to foster the completion and sound enhancement of such technical concepts. Developing and ideally piloting such kind of functional prototypes as well as implementing specific digital workflows in a transparent way will help to move the discussion from a theoretical to a more implementation-oriented and practical angle.

7. Conclusion

This publication highlights the transformative potential of Distributed Ledger Technology (DLT) and the use of Smart Contracts with the aim of redesigning financial instruments and associated processes, particularly in the wholesale bond market. The introduction of the eWpG in Germany has provided a legal framework to replace traditional processes with innovative digital solutions. The holistic integration of asset tokenization and digital payment infrastructures in the form of a standardized functional protocol opens new potential for optimizing the issuance process and the overall life cycle in general. With the SBC concept we aim to actively contribute to the discussion regarding development of open digital standards, thereby fostering the development of innovative digital interaction protocols in a transparent and expandable way. We invite other institutions to collaborate with us in reviewing and enhancing our approach.

Further Reading

[1] BIS Innovation Hub and N.Y. Federal Reserve Bank, “Project Pine - Central bank open market operation with smart contracts,” 05 2025. [Online]. Available: https://www.bis.org/publ/othp95.pdf.
[2] KfW and KPMG, "DLT-based capital market – An analysis of the degree of maturity based on KfW's first two blockchain-based digital bonds," Februar 2025. [Online].
[3] F. Vogelsteller and V. Buterin, “ERC-20: Token Standard,” Ethereum Improvement Proposals, [Online]. Available: https://eips.ethereum.org/EIPS/eip-20.
[4] Monetary Authority of Singapore, “Guardian Fixed Income Framework,” 2024. [Online]. Available: https://www.mas.gov.sg/schemes-and-initiatives/project-guardian.

[10] Ebers, Keyword Commentary Legal Tech, Smart Contracts para. 7
[11] Ebers, Keyword Commentary Legal Tech, Smart Contracts para. 10

[5] ECB, "Sound Practices for Managing Intraday Liquidity Risk," November 2024. [Online]. Available: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.Sound_practices_for_managing_intraday_liquidity_risk_202411~aec6d34ffa.en.pdf.

[6] C. P. Fries and P. Kohl-Landgraf, "ERC-7573: Conditional-upon-Transfer-Decryption for DvP," Ethereum Improvement Proposals, 5 December 2023. [Online]. Available: https://eips.ethereum.org/EIPS/eip-7573.

[7] C. P. Fries and P. Kohl-Landgraf, "A Stateless and Secure Delivery versus Payment across two Blockchains," 2023. [Online]. Available: https://ssrn.com/abstract=4628811.

[8] R. La Rocca, R. Mancini, M. Benedett, M. Caruso, S. Cossu, G. Galano, S. Mancini, G. Marcelli, P. Martella, M. Nardelli and C. Oliviero, "Integrating DLTs with Market Infrastructures: Analysis and Proof-of-Concept for Secure DvP between TIPS and DLT Platforms," Banca d'Italia, 2022. [Online]. Available: https://www.bancaditalia.it/pubblicazioni/mercati-infrastrutture-e-sistemi-di-pagamento/approfondimenti/2022-026/index.html.

Impressum

DZ BANK AG
Deutsche Zentral-Genossenschaftsbank,
Frankfurt am Main
Platz der Republik
60325 Frankfurt am Main
Postanschrift
60265 Frankfurt am Main
Telefon: 069 74 47-01
Telefax: 069 74 47-16 85
www.dzbank.de
mail@dzbank.de
(Bitte keine unverlangte Werbung und keine Aufträge per E-Mail:
Siehe Hinweise zur E-Mail-Kommunikation unter "Rechtliche Hinweise".)
SWIFT-Code/BIC-Code: GENO DE FF
BLZ: 500 604 00

Vertreten durch den Vorstand:
Dr. Cornelius Riese, Vorstandsvorsitzender
Souâd Benkredda
Uwe Berghaus
Dr. Christian Brauckmann
Ulrike Brouzi
Johannes Koch
Michael Speth
Thomas Ullrich

Aufsichtsratsvorsitzender:
Henning Deneke-Jöhrens

Sitz:
Eingetragen als Aktiengesellschaft in Frankfurt am Main, Amtsgericht Frankfurt am Main, Handelsregister HRB 45651

Aufsicht:
Die DZ BANK wird beaufsichtigt durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und die Europäische Zentralbank (EZB).

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Graurheindorfer Str. 108
53117 Bonn
http://www.bafin.de

European Central Bank (ECB)
Sonnemannstrasse 20
60314 Frankfurt am Main, Germany
http://www.ecb.europa.eu/home/html/index.en.html

Umsatzsteuer Ident. Nr.:
DE114103491

Verantwortlich für den Inhalt:
Peter Kohl-Landgraf (Capital Markets Trading)
Henning Ahmann (Capital Markets Institutional Clients)
Nico Braun (Fixed Income Syndicate)
Julian Eicke (Security Services & Digital Custody)
Christian Fries (Group Risk Control)
Martin Kötter (Capital Markets Trading)
Nicole König (Group Treasury)
Frederick Spahn (Group Treasury)

DZ BANK AG
Deutsche Zentral-Genossenschaftsbank,
Frankfurt am Main
Platz der Republik
60325 Frankfurt am Main

www.dzbank.de