Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche
Kreditwirtschaft

Working Paper on Commercial Bank Money Token

Version 1.5 (March 6th, 2023)

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Jens Holeczek
Associate Director
E-Mail: j.holeczek@bvr.de

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German Banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the publics, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
Bundesverband der Deutschen Volksbanken
und Raiffeisenbanken e.V. (BVR)
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
www.die-deutsche-kreditwirtschaft.de
www.german-banking-industry.org

Supporting Associations:

Bundesverband
der Deutschen Volksbanken
und Raiffeisenbanken · BVR

bankenverband

Finanzgruppe
Deutscher Sparkassen- und Giroverband

VÖB die öffentlichen Banken

Other associations are more than welcome to support the concept of commercial bank money tokens and/or participate in the development of the concept.

Content

Table of Figures

Change History

Changes			
Date	**Version**	**Author**	**Comments**
05.12.2022	1.3	DK	▪ Publication of the first version of the CBMT concept
06.03.2023	1.5	Working Group	▪ Solution for "Travel Rule" obligations ▪ New chapter "Supporting multiple currencies" ▪ Introduction of blacklist ▪ Adjustments in form of sharpening address properties and new clear diagrams

Abstract

The German Banking Industry Committee (GBIC) first explored the potential of a Commercial Bank Money Token (CBMT) in a Whitepaper published in July 2021.[1] We have now detailed some aspects to further explore the potential of a CBMT. This working paper contains our conclusions on this topic and represents our contribution to the current discussions on tokenized money.

We are pleased to enrich these discussions with this contribution and to point out possible solutions for the realisation and implementation of multi-issuer concepts, which can be an important basis for the further discourse. Therefore, we invite interested parties to further contribute on the subject and to reach out to the GBIC and the working group to discuss the several aspects.

Additional notes on this version of the working paper:

- The paper is based on several assumptions, among other things that a CBMT mainly addresses industry needs. However, the CBMT could conceptually serve Retail DLT use-cases as well.
- The current legal framework for commercial bank money is only partially covering the aspects of a CBMT and must be further developed while the alternatives like the E-Money-Regulation or MiCAR do not apply. For such regulatory evolution, it is of high importance to provide a detailed understanding, how a CBMT must work from our point of view.
- Several aspects described in this paper are still high level as we aim to create the design technology-agnostic. However, the technical design on a specific DLT framework will need to provide more detailed solutions to technical feasibility, legal and regulatory requirements, and operational needs (for example integration into bank's legacy systems).
- As a next step the Working Group aims to implement such design on a specific DLT framework together with industry partners to demonstrate the feasibility of a CBMT solution and to create more insights on technical, legal, regulatory, and operational needs.

In our Whitepaper on an ecosystem of CBDC, tokenized commercial bank money and trigger solutions, we stated that a CBMT shall be designed complementary to a Retail-CBDC, which is currently under investigation within the digital euro project of the ECB.

Additionally, CBMT should be the answer of the banking industry on stablecoins issued by non-banks. Given that retail CBDCs might address different use cases than blockchain-based settlement assets, we see an increased competition in stablecoins / e-money tokens.

We want to highlight that we still believe in the necessity of this ecosystem that covers the market's needs in payments for retail and wholesale customers. A digital euro consisting of CBDC, CBMT and regulated stablecoins can help to reach the proclaimed policy objectives as well as build a strong and resilient base for the currency euro in the worldwide competition.

[1] Europe needs new money – an ecosystem of CBDC, tokenized commercial bank money and trigger solutions, https://die-dk.de/media/files/20210625_DK_Ergebnisdokument_EN.pdf

1. Executive Summary

Banks and financial intermediaries are important partners for the financing of the industry and the development and growth of the national economies. Banks support commercial processes as trusted third parties to facilitate and process the transfer of money for decades now and have thereby established as an important partner in payments. They have built very efficient, large and secure networks based on sophisticated clearing & settlement mechanisms to ensure a trusted and secure payment processing. These are also based on so called "commercial bank money", a direct liability against a commercial bank. However, commercial banks ensure that commercial bank money is 1:1 convertible to central bank money at any time and furthermore also partly secured through statutory deposit protection schemes.

Although currently existing forms of money work quite well with available payment systems, there are technological developments that have shaped new requirements that existing solutions do not cover adequately. For example, the industry is currently experiencing a digital transformation - also called Industry 4.0 - which involves extensive process automation through the usage of DLT (Distributed Ledger Technology), smart contracts and microtransactions. However, existing payment solutions based on the available forms of money are not suitable for this. CBDC or stablecoins issued by non-banks can be a threat to the current financial system. So while providing a state of the art means of payment for important DLT-based industry processes the CMBT also prevents a disintermediation in today's financial system.

In order to meet these new requirements, commercial bank money as it is available today must adapt to the same technologies as the industry 4.0. So it can become an inherent part of industry's business value chains and to leverage the potential of the technology in the banking sector. This new technological representation of commercial bank money is called "Commercial Bank Money Token" (CBMT). A CBMT still represents commercial bank money with all its features and services provided by banks but might enable new and additional functionalities leveraging DLT.

- A CBMT can provide the best possible value if
  - it is made available directly on Industry DLTs (CBMT is multi-DLT capable),
  - agnostic of wallet owners and payment processors and
  - the clearing & settlement mechanisms between banks are fully transparent (CBMT is a multi-issuer concept).
- However, it is conceptually possible to use an interbank DLT network for the CBMT issuance as well.
- Banks are leveraging a Technical Service Provider, the so-called TSP, which does not include the money of banks and clients in its own balance sheet for token mining and as the contractual counterpart for the industry. This discussion paper describes the role and the tasks of the TSP as well as provided services.
- Banks remain responsible to ensure regulatory compliance of payments, in respect of KYC, AML or CFT checks. This paper also describes a target image for them in the CMBT ecosystem.
- This paper also describes the token life cycle and transaction processes in detail.
- To ensure a stable and resilient payment system for the industry, the Working Group not only defined a common standard for the realization of the token but also drafted first suggestions on how to deal with unhappy events.

2. Introduction - Why do we need a Commercial Bank Money Token?

With the inherent trust and security of DLT, the role of banks in maintaining payment networks might be questioned, while the commercial bank money as widely trusted money form remains. Today's commercial bank money serves as a model for the development of tokenized commercial bank money by guaranteeing convertibility and fungibility. Commercial bank money also fits in the existing system of financial bookkeeping at banking clients.

The focus of the CBMT should be on supporting the ongoing digitalization of business processes in Industry 4.0 in a timely and effective manner, but also on the rapidly growing importance of digital assets and the digitalization of international transactions. The CBMT would be applicable as a further development of today's commercial bank money on the base of DLTs and would enable a flexible supply of liquidity to the economy while keeping the possibility of commercial bank money creation. In this way, the CBMT would focus on the needs of businesses, whereas the current discussion about the digital euro issued by the ECB focuses primarily on the requirements of consumers.

Maintaining commercial bank money is also particularly important for the stability of our two-tier money system. So far, the design choices prioritized by the ECB indicate that the digital euro discussed by the ECB will not meet the needs of private and corporate customers in the same way. Since a digital euro by the ECB will probably focus on retail use-cases, it does not necessarily match the needs of the industry for the integration of payment transactions regarding process automation using blockchain technology. In any case, an excessive reduction in the amount of commercial money would limit lending and endanger the two-tier money system.

With respect to the political and economic implications of a digital euro (impact on bank deposits, disruption of existing payment solutions etc.) a CMBT would strengthen commercial bank money and therefore also the two-tier money system while meeting today's corporate customers demands. In this paper, the GBIC introduces a possible concept for CBMT to support the digitalization of the industry, especially in context of upcoming DLT-based industry platforms.

Today we already see examples of digital business processes supported by tokenized money. They are either based on using cryptocurrency, stablecoins or a token issued by one bank in its own ecosystem. While tokenized commercial bank money can be issued by any bank in its own ecosystems, the real benefits come with a multi-issuer concept in which commercial bank money tokens are fully fungible and convertible to both traditional commercial bank money and central bank money.

A CBMT aims to support DLT-based business processes. Currently, these business processes are mainly explored by the Industry as B2B use-cases. Examples for such business processes are:

(1) Delivery-versus-Payment (DvP) use-cases in Supply Chain Finance, Trade Finance and Securities Settlement
(2) Pay-per-Use cases
(3) Smart contract-initiated payments and deep integration of payments into process flows

(4) Continuous payment streams

Having tokenized commercial bank money directly on industry DLTs could create boost for optimizing DLT-based (B2B-) use-cases. This enables instant, secure and cheap transfers of money as an integral part of the value chain. Therefore, it is part of the CBMT concept to issue CBMT on industry blockchains.

3. Challenges of a Commercial Bank Money Token

3.1 Design related obstacles

There are several challenges for CBMT that need to be addressed and discussed within the conceptual framework. These obstacles shall be solved through the design for the processing of CBMT.

Clearing & Settlement mechanism (CSM)

With the multi-issuer concept of CBMT, the challenge of clearing and settlement of CBMT receivables and liabilities between banks must be solved. In the traditional commercial bank money system, Clearing and Settlement (CSM) happens in central bank money and are processed by the Central banks. We expect this mechanism to be used for CBMT as well. In a later stage of this initiative, it might be useful to introduce a direct bilateral/multilateral clearing mechanism on the industry DLT.

Multi-Issuer/Multi-DLT concept

The management of serving a number of industry DLTs with CBMT together with other issuing banks requires:

- Management of Nostro-addresses (wallets) on industry DLTs incl. risk/limit management and related CSM
- Specific processes to ensure regulatory and internal compliance using CBMT

New Market issuance and Market exit

The CBMT shall be made available on industry DLTs. These are usually built as private blockchain applications to address specific industry use-cases, created as value chain driven platforms between few corporates. This means that there are a significant number of DLT-based platforms that are probably in need of a CBMT. It is of importance to have a simple and fast onboarding process for industry blockchains to allow them using CBMTs easily.

As banks take the risk to issue and accept CBMT the same way as commercial money, they need to have full control over this type of money. This includes the possibility for the issuing banks to cancel the issuance and acceptance of CBMT on industry DLTs in case of potential misuse of CBMT hampering banks in fulfilment of their regulatory obligations or in case of the termination of contracts between a bank and its customer.

3.2 Regulatory and internal compliance

There are several regulatory obligations to be respected when designing and implementing a CBMT:

- **Know-your-Customer (KYC)**: It has to be ensured that transfer of CBMTs is only possible with trusted parties, i.e., which are known by the banks issuing/accepting CMBTs.
- **Countering-the-Financing-of-Terrorism (CFT) and Financial Sanctions**: A payment transaction must be checked against AFC/Sanctions before finalization of the payment settlement. As a transfer of CBMT from one wallet to another is "just" a transfer between wallets (addresses on the DLT) with immediate finalization (in contrast to today's sequential account-based settlement), a check for CFT/FS is rather complex, especially as banks maintain differing internal policies whether to execute such transactions.
- **Anti-Money-Laundering (AML)**: Payment transactions are ex post regularly analysed for suspicious patterns regarding AML. This is probably only possible if banks have access to customer CBMT addresses and/or related transactional information, for example via a permissioned DLT network with whitelisted network participants agreeing to such transaction pattern analyses.
- **Fraud Protection**: A payment transaction should be checked against fraud patterns before finalization of the payment settlement. As a transfer of CBMT is a transfer between addresses with immediate finalization, a check for potential fraud is rather complex. But such transfer is only valid in case, both sender and receiver addresses are whitelisted by one of the issuing banks. Therefore, it can be expected that fraud is hardly possible.

As a result of the compliance-related requirements, the best way forward is to ensure a continuous screening of addresses (i.e., persons with access to the cryptographic keys of addresses, that is wallet owners) of the industry DLT, i.e., to continuously monitor the whitelist provided by the Technical Service Provider. Issuing banks must agree on a common framework which addresses to accept. In future, additional apps could be built on top of the network that enable a joint and more efficient approach to CFT, AML and fraud e.g., a pre-validation process, where each bank would do the checks automatically and after that, the payment is initiated.

3.3 Legal Framework

3.3.1 Legal positioning of CBMT

We believe that a Commercial Bank Money Token needs to be seen as commercial bank money in an alternative technical form, i.e., not provided as electronic money on current accounts but as digital money provided on token accounts ("addresses"). It should thus follow the same regulations. Two major issues need to be considered in this respect today:

1) There is no commercial bank money regulation that could be adjusted to reflect the idea of tokenized commercial bank money.
2) Several current regulations in context of so-called crypto assets might affect the creation of a Commercial bank Money Token on DLT.

Several areas need to be considered when discussing regulatory changes for CBMT:

- **Deposit protection**: CBMT need to fall under deposit protection schemes, the same way as today's commercial bank money (e.g., Directive 2014/49/EU, deposit insurance law, deposit insurance fonds for specific banking sectors)
- **Payment initiation by software and 2-factor authentication**: Industry DLT platform partners want to create own (business and payment) rules using smart contracts. This includes rules for initiating payments using bearer instruments. Current regulation requires a human interaction and a 2- factor authentication (e.g., PSD 2)
- **No E-Money token**: MiCA-regulation explicitly excludes (account-based) deposits (as defined in Article 2(1), point (3), of Directive 2014/49/EU), but not tokenized deposits. At the same time, it regulates E-Money Token which might capture tokenized commercial bank money (see MiCAR and amending Directive (EU) 2019/1937 Art. (3), (2) and (4)).
- **"FATF Travel rule / Transfer of Fund Regulation"** might apply as well. The adaption of the Transfer of Funds Regulation is not yet finalized. The CBMT solution would store information on the "whitelist" about the DLT address-owner with all information required to meet the Travel Rule obligations. The Technical Service Provider will enrich any transactional data queries with this additional data in case needed.
- **VAT (Tax Transparency) Regulation** might apply as well even if it is hardly possible to identify cross-border transactions on an industry blockchain with CBMT. The issue needs to be discussed with the Regulators.
- In addition, and also from an accounting perspective, CMBT should be treated **like sight deposits** – on the balance sheet of the issuing bank, but also on the balance sheet of the holding customer.

CBMT is another form of commercial money (see Figure 1 for a comparison with traditional forms of money) that has not yet been found in the existing laws and regulations. It may be necessary to discuss sharpening the scope and definitions of existing rules and regulations and/or develop new provisions.

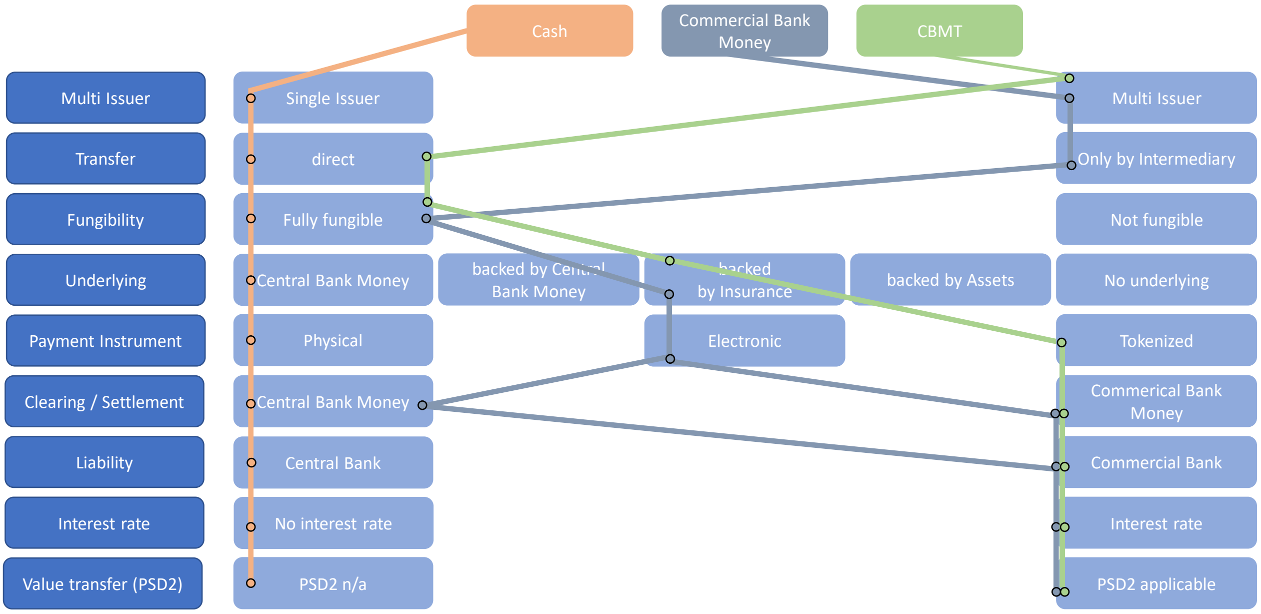


Figure 1: Comparison main features of cash, commercial bank money and CBMT

3.3.2 Regulation on information accompanying transfers of funds and certain crypto assets

The 2020 Action Plan of the Commission includes as proposal for the recast of Regulation EU 2015/847 expanding traceability requirements to crypto assets. The Commission justifies its proposal to the effect that "transfers of virtual assets have remained outside of the scope of Union legislation on financial services". To ensure the coherence of the EU legal framework, this regulation will use the definitions of 'crypto-assets' and 'crypto-asset services providers' (CASPs) laid down in the Commission proposal for a regulation on Markets in Crypto-assets (COM (2020)593 final). The CBMT is positioned very similar to the existing commercial money and no crypto asset in the meaning of the regulation on Markets in Crypto assets.[2]

The CMBT also not corresponds to the definition of "virtual assets" set out in the recommendations of the Financial Action Task Force (FATF)[3]. "Virtual Assets" are defined by FATF, "as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes.

[2] References to MiCAR to be added once the text adopted

[3] FATF International Standards on Combating Money Laundering and the Financing of Terrorism (as amended in October 2020): (http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf)

Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations".[4]

Article 4 Definitions of the Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market ("PSD2") defines "strong customer authentication" (SCA) as:

"(30) an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data".

Article 97(1) lays down the scope of the SCA:
"Member States shall ensure that a payment service provider applies strong customer authentication where the payer:

a) accesses its payment account online;
b) initiates an electronic payment transaction;
c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses".

The transfer of CMBT is neither an online access to a payment account nor the initiation of an electronic payment. Payment transaction means: "an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee" (Article 4 (5)).

On a top level in a DLT world the "payer"/"payee" is known, but in the context of the PSD2 a payer is a natural or legal person who holds a payment account (Article 4 (8)). A DLT machine-to machine world is not payment account based and only technical addresses are acting instead of natural or legal persons.
A payment order in the meaning of PSD2 is not initiated ("payment order"' means an instruction by a payer or payee to its payment service provider requesting the execution of a payment transaction", see Article 4 (13)).

DLT is no remote channel within the meaning of the directive: "initiated via internet or through a device that can be used for distance communication;" (see Article 4 (6)).

All in all, the essential features for the application of PSD2 to the transfer of CMBT in the DLT are missing. Article 97 is therefore not applicable and no exemption under Article 17 is required. This should be legally confirmed.

[4] see: page 11, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast), COM(2021) 422 final 2021/0241 (COD).(https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52021PC0422)
see: page 13, nr. 33 GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html)

3.3.3 The CBMT as a PSD2 payment instrument

As per PSD2 Article 14 (14)[6] payment instrument means "a personalized device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order". A CMBT token may possibly be considered as a "set of procedure".

In Annex I of the directive any payment services referring to point (3)[5] of Article 4 ("business activity") are listed:

- Cash placed /withdraws on/from a payment account: Not applicable.
- Direct Debits or credit transfer: Not applicable
- Issuing of payment instruments and/or acquiring of payment transactions: services based on specific payment instruments that can be used only in a limited way are excluded as per Article 3 (k).
- Payment initiation services: Use of CMBT is no initiation of "a payment order at the request of the payment service user with respect to a payment account held at another payment service provider" (Article 4 (15)).
- Account information services: Not applicable
- Money remittance means as per Article 4 (22):" payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee."

Money Remittance can be based on cash provided by a payer to a payment service provider which is transferred via a network to a payer. While the CMBT is a personalized instrument, it is not used with a payment service provider, and it is more like cash. Classifying the CBMT as a PSD2 money transfer instrument is beneficial since the token is then not e-money.

3.3.4 New and additional regulations

While the current commercial bank money is managed by banks only which have full control on all deposits and transactions, a CBMT is managed partially by the bank and partially by the Industry DLT. Even if banks are able with the a.m. concepts to keep control on CBMT and ensure regulatory compliance in the current legal framework, new and additional regulations might be developed to clarify better responsibilities and liabilities in a distributed ledger environment.

[5] DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

4. Design Principles of a Commercial Bank Money Token

The CBMT must have various functionalities and map the consolidated customer requirements and needs. A key aspect of the CBMT is interoperability. A distinction is made here between four dimensions of interoperability:

- Interoperability with existing forms of money, especially with deposit money (convertibility).
- The interoperability between CBMTs issued by different institutions (fungibility).
- The interoperability between CBMTs issued on different DLTs.
- The interoperability between CBMT and payment initiation systems (e.g., smart contracts).

To exclude counterparty risks and ensure the token's universal applicability, all four forms of interoperability must be guaranteed. Consequently, future tokenized commercial bank money needs to be fungible between commercial banks and savings banks and – bearing in mind existing limits – it must be convertible to today's commercial bank and central bank money (cash, in the medium term also CBDC).

To achieve the interoperability and lead the CBMT to represent a claim against the issuing commercial bank in the same way as commercial bank money, we need to define a few more main aspects.
These are split up into technical, bank-specific and general aspects:

4.1 Technical Aspects

- We aim to be able to issue the CBMT on any DLT framework that supports a set of features.
- The banks designate a joint technical service provider (TSP) that takes care on the definition of token standards and the issuance of blank tokens and allows different interfaces for the access.
- A 24/7 availability of CBMT must be ensured.
- It is possible to use CBMT offline, however with the requirement to regularly be updated online; it is possible to limit the amount (this is based on the properties of today's cash and electronic payment transactions). See chapter 7.7.1 for more details.
- There should be no programmability of the token (in the form of inherent properties) and a possibly associated purpose of limitation since the universality as a monetary property is then possibly no longer fulfilled and differing economic values due to different risk profiles between the deposit tokens are excluded.
- However, due to the programmability of the underlying infrastructure, individual functionalities (including smart contracts) can be assigned to a CBMT. In this way, only the payment is programmed and the monetary unit in the form of the CBMT can still be used confidently and universally (preservation of fungibility).
- The CBMT runs on a DLT, so that the transactions are always finalized instantly, and the transaction speed of the deposit tokens should be achieved (at least) in seconds.
- Corporate customers should be involved regardless of whether they run their own or participate in some DLT.

- The DLT must be able to restrict the transfer of CBMT to smart contracts written by the TSP. This is necessary so that all transfers of CBMT are subject to the rules for CBMT – either checking the whitelist or adding to the history of owners of a token.
- As the tokens are scriptural money, the token must be able to record the issuer. See 5.5.4 for the minting process.
- For transferring tokens, a smart contract must be mandatory that checks all involved addresses against the whitelist. This is necessary to ensure compliance with the purposes of the whitelist, that is, AML, KYC and other regulatory or contractual restrictions.
- A second, optional smart contract for token transfers should also be offered, which allows the transfer of tokens between addresses without consulting the whitelist. This transfer needs to record the history of addresses as a set and allows a limited number of transfers. See chapter 7.7.1 for details on the use of this smart contract. The history is cleared if such a token is transferred using the smart contract that consults the whitelist.

4.2 Bank-specific Aspects

- A collateralization of the CBMT – at least in line with the Basel IV requirements – is secured in the same way as for account-based commercial bank money today.
- The redemption of CBMT is only guaranteed for transfer between trusted addresses. A list of trusted addresses will be provided by the issuing/accepting banks of CBMT. See chapter 5.2. If CBMT is transferred to untrusted addresses the redemption is subject to AML and KYC. (See chapter 7.7.1).
- The interoperability should either be built up via APIs or made possible through direct and native issuing on the blockchains of corporate customers.
- A confidentiality towards third parties in accordance with the regulatory requirements (e.g., within the framework of banking secrecy and AML / CFT compliance) must be ensured like today's audits and regulations of commercial bank money.
- An anonymity of the customer in the context of the CBMT can be largely ruled out against the background of existing AML requirements. A possible approach for this, however, would be the link with amount limits per customer. The provision of anonymous payments using the deposit token could be useful and desirable if a CBDC issued by the ECB does not cover this function but must be technically evaluated.
- Commercial and savings banks should agree on a joint technical service provider that defines common token standards and is responsible for issuing tokens (see chapter 5).
- Deposit Protection Scheme – Although it is of limited interest for (large) corporations, the CBMT should be part of the deposit protection scheme in the same way commercial bank money is today.

4.3 General Aspects

- It should be possible to set the CBMT in any part and any amount from sub-cents to large amounts.
- Only customers who have an account with the issuing bank should be able to exchange CBMT, additional contractual conditions to be agreed.

- A customer of a bank must at any time have the right to exchange a CBMT from another bank to a CBMT of its house bank. This right is a condition for the fungibility and uniformity of all CBMT and reflects today’s situation, where the commercial bank money account is held with the bank, the customer has chosen a priori.
- For the implementation of accounting and compliance aspects of banks, the immediate exchange of CBMT to the customers house bank is expected to happen.

4.4 Addresses used by the participants

In this document, we use address types with different functionality for customers and banks. Customers have at least two addresses, while banks have four.

4.4.1 Customers Addresses

A customer will have at least two addresses: the general and the convert address.

- Convert address – The convert is the inbound address of the customer. Tokens sent to the convert address will automatically be converted and forwarded to the associated general address.
- General address – The general is the outbound address of the customer. Sending tokens is always performed from the general address.

4.4.1.1 Properties of the Convert Address

- A customer can have one or more convert addresses.
- Each convert address must be associated to exactly one general address.
- Convert addresses do not store tokens.
- The convert address should be the default address that the customer specifies as the receiver address with their business partners.
- A convert address can be associated with one or multiple banks from the set of banks that have whitelisted the general address the convert address is associated with.
- For each convert address, the customer must explicitly specify the “preferred issuer” and “preferred currency” as mentioned in the algorithm in chapter 6. This preferred issuer will be called “house bank” in the following.

4.4.1.2 Properties of the General Address

- A customer can have one or more general addresses.
- General addresses must be associated with at least one bank (multiple banks are possible).
- General addresses store the tokens of associated banks.
- The customer basically holds the keys of the general address. However, we expect Banks to offer hosted wallets to maintain the private keys.
- For some special use cases like intra-group payments, it may be useful to use the general address as receiving address. In this configuration no conversion as described in 6.4.2 takes place. Using the general address as receiving address entails certain risks and is not advised.

4.4.2 Bank Addresses

Banks will have four addresses for every supported DLT:

- Issuing address - used by the bank to receive the blank token from the TSP.
- Mint address – the minted tokens are sent to the mint address and from there sent to the customer's address.
- Redemption address - used to receive inhouse CBMT after the settlement and for redemption by customers.
- General address – used to hold foreign bank tokens (tokens from another bank).

5. A Technical Service Provider as central partner for Commercial DLT Providers

5.1 Tasks of the TSP

CBMT issuing/accepting banks will leverage a TSP to support the introduction of CBMT on specific Industry DLTs. The TSP is the technical interface for the bank and industrial customers. So, the TSP must have interfaces for industrial customers with different DLTs, also banks with different DLT and interfaces (e.g., API) for banks without a DLT. The technical service provider is responsible for:

- Contracts between the Industry DLT provider and the CBMT banks. Such contracts are required to ensure:
  - All addresses that are used for payments are properly known, i.e., validated and certified by banks (providing a "whitelist" of validated addresses) or other regulated institutions.
  - Rules/services for transaction authorization.
  - A possibility to terminate the issuance/acceptance of CBMT by banks in case of misuse or moratorium.
  - An agreement of limits for CBMT managed on the commercial DLT.
  - Access to customers CBMT addresses by the account-holding banks (read-only to ensure regulatory compliance or possibility to initiate specific types of transactions like token exchange).
  - Maintenance of Technical Service Provider and bank addresses on Industry-DLT.
- Programming / verifying the smart contracts for transferring CBMT. Only allow new smart contracts if they have been checked for guidelines and accuracy.
- Providing the whitelist of allowed CBMT addresses (for detailed information see the next section).
- Mining of CBMT - The TSP is the only entity technically capable of creating tokens and publishing them on the Industry DLT.

- The transfer is only possible between "white-listed" addresses. Even if it should be prevented by smart contracts, in the unwanted case of an unauthorized transfer of CBMTs or a transfer to a non-authorized address, the CBMT loses its connection to the issuing bank, i.e., the claim against the issuing bank.
- Burning CBMT - Tokens are only burnt by the TSP. Only the issuing bank can instruct the TSP to burn tokens that it holds in its custody. Only from there tokens can be transferred to the TSP for burning. The following approaches were considered:
  1. Burning CBMT when a customer is offboarding or when the customer wants to change CBMT into commercial bank money. This is better done by swapping the tokens for money with the bank of the customer. The bank then swaps the foreign tokens with the other bank.
  2. Burning CBMT when a bank does not want to participate anymore. The bank that wants to leave burns its own tokens, as described above.
  3. Burning CBMT when a Bank A Token is changed to Bank B Token or vice visa (A token of Bank A can only be burned by Bank A. So, if the transfer is completed at Bank B a Smart Contract must be started that will burn the Token at Bank A.)

5.2 Conditions of a Whitelist

The whitelist is a list of all allowed CBMT addresses and must fulfil the following requirements:

- The TSP is the owner of the whitelist and is the only one that can include or exclude addresses from the list.
- The banks report the addresses they have whitelisted to the TSP.
- The banks can send mandatory requests for exclusion of their own customers.
- Each CBMT issuer provides an oracle for querying the trust status of an address.
- Every participant of a DLT can request the trust status of an address for that DLT. Especially every bank can check the addresses against the whitelist.
- The whitelist contains the owner of an address including owner name and full address according to the Travel Rule requirements as well as information about the banks and currencies for which a relationship of the address can be used to hold tokens.

5.3 Conditions of a Blacklist

Each bank can register addresses for their own blacklist. Tokens issued by the blacklisting bank can't be transferred to any address on the blacklist of that bank (e.g., due to embargo issues). A blacklist is created to protect the bank from "unwanted" recipient addresses. The blacklist is bank-individual and for another bank or customer not viewable. Reasons may be exclusion from business activity due to internal requirements (e.g., prohibition of participation in gambling), different national sanction lists or moratorium/insolvency of the recipient. The assignment of this addresses to the legal name of the unwanted recipient presents a challenge.

Tokens can’t be issued and transferred by the blacklisting bank to any address on the blacklist of that bank. Other banks can continue, i.e., if client X is on the blacklist of bank A but not blacklisted in bank B and Z, the client X can continue to send tokens from B to Z and from Z to B.

5.4 Establishment of the TSP

There are two options when it comes to establishing the TSP. Either the banks join forces and jointly establish a TSP. This would have the disadvantage that it could not be implemented quickly and would involve many coordination hurdles. Another option would be to involve an existing third party. This would involve the risk that the third party may pursue its own interests, but it would at least be an option to launch CBMT as soon as possible.

5.5 Token Cycle

The approach of implementing a Technical Service Provider (TSP) that does not have its own balance sheet allows banks to maintain the commercial bank money creation without shrinking their balance sheets. The following part explains and illustrates the process of mining, minting, converting, transferring, de-minting, and burning of CBMT.

The token cycle of CBMT is explained by taking Bank A and Bank B as examples. As a simplification, we assume that only one currency is in play and furthermore that each token corresponds to a value of 1 €. The FX case is described in detail in chapter 6.

5.5.1 Overview of the Token Cycle

To get a first glimpse of the cycle, Figure 2 provides a brief overview of the cycle between a customer and his bank on the industry DLT. This and more complex cases will be detailed in the next chapters. The Token Cycle in general contains the following parts:

- The customer requests token for commercial money
    - the bank needs to request blank tokens from the TSP (if there is not already enough on the issuing address)
    - the bank mints the token
    - when the bank sends the token to the customer, the token will be credited to the customer, commercial bank money debited.
- When the customer wants to change the token back into commercial money
    - the money will be de-minted

- the bank can burn the token afterwards.

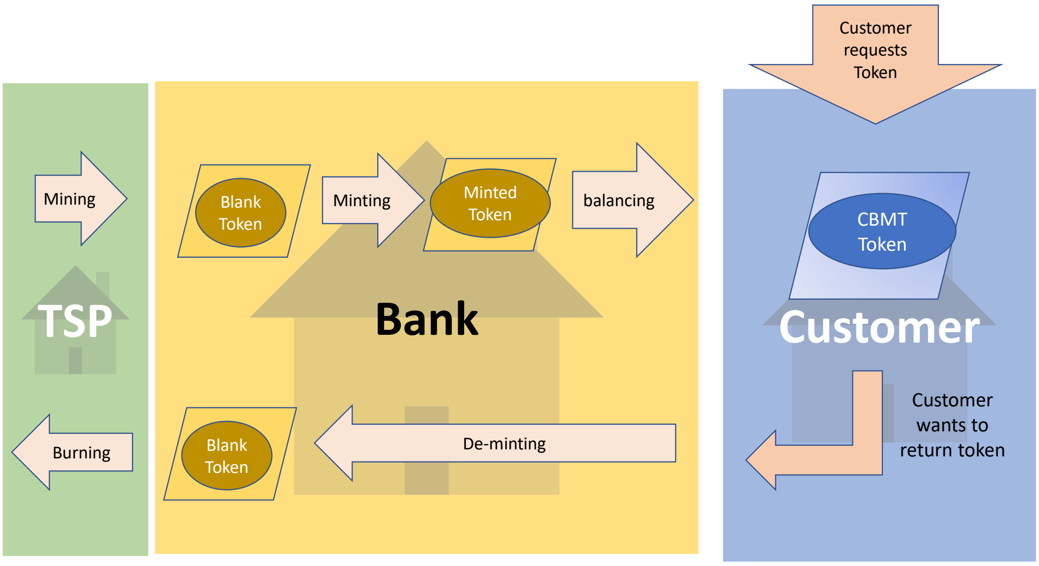


Figure 2: Overview of Token Cycle

5.5.2 Mining and Minting

We introduce the concept of minting to mirror the process used in the issuance of commercial papers for accounting. There is no technical requirement for this concept, but it makes arguing about the accounting easier.

When issuing commercial papers, the complete notional of a paper is credited to the issuing account. The documentation for the issuance also is created for the complete notional. The issuing account is not included in the balance sheet. Only when the commercial paper is sold out of the issuing account and credited to the buyer, the amount that was sold is included in the balance sheet.

The separation between "mining" and "minting" mirrors this distinction to keep the similarity in accounting. The mining of tokens provides the bank with the technical ability to credit the tokens to customers. The amount of mined tokens on the General Address of the bank mirrors the amount on the issuing account for commercial papers.

The minting of tokens combines the crediting to customers and the inclusion in the balance sheet. This mirrors the selling of commercial papers from the issuing account to the buyer. Similar reasoning leads to the existence of de-minting and blank tokens. This separates de-minting and burning. We are not certain that this step is necessary, but we keep it for symmetry reasons.

5.5.3 Mining of blank tokens

The mining process starts with the bank's demand for CBMT – in this case Bank A's demand – and the subsequent instruction to the TSP to mine them. The TSP mines the blank tokens and sends them to Bank A's issuing address (see Figure 3 Mining of blank tokens). Only the TSP is technically capable of programming and defining the scheme of tokens to make them a fungible representation of today's commercial bank money. Although, the tokens have the technological parameters of CBMT, at this point they have no value, because the TSP does not have its own balance sheet and the tokens are not yet backed by a bank's claim or by assets held. That's why we call them "blank" tokens - they are, in a sense, the "blank shell" of tokens.

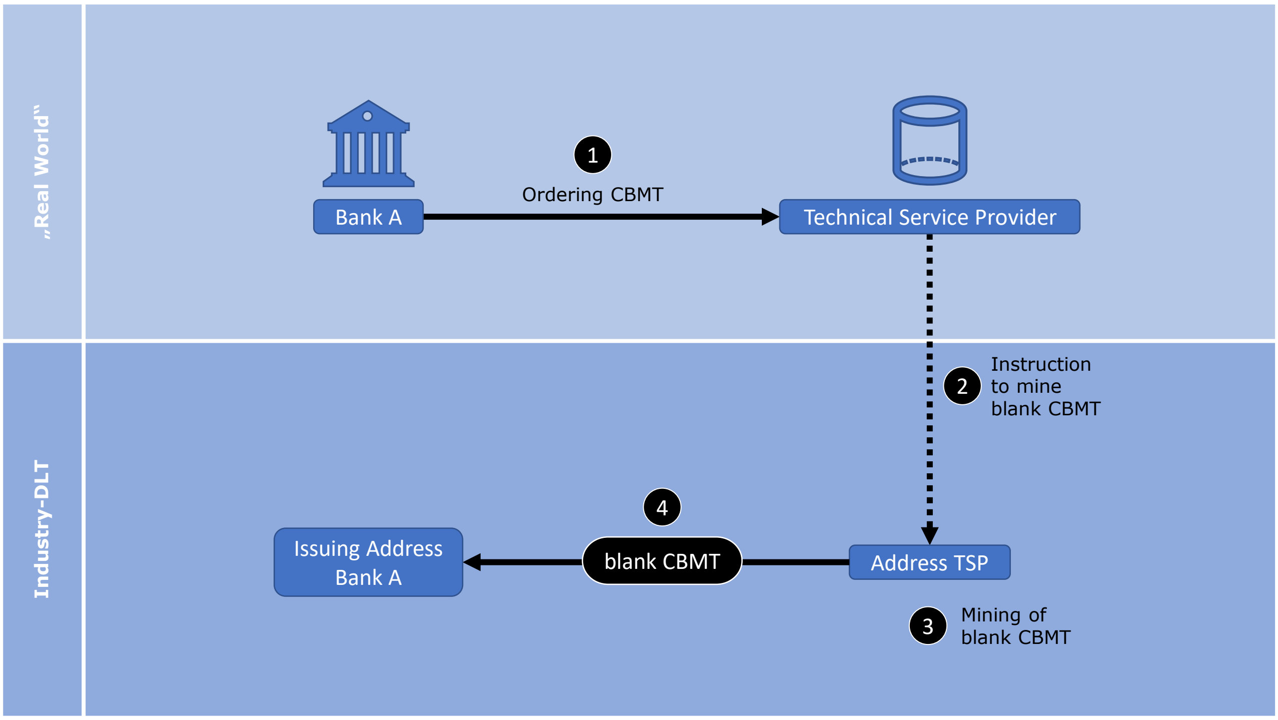
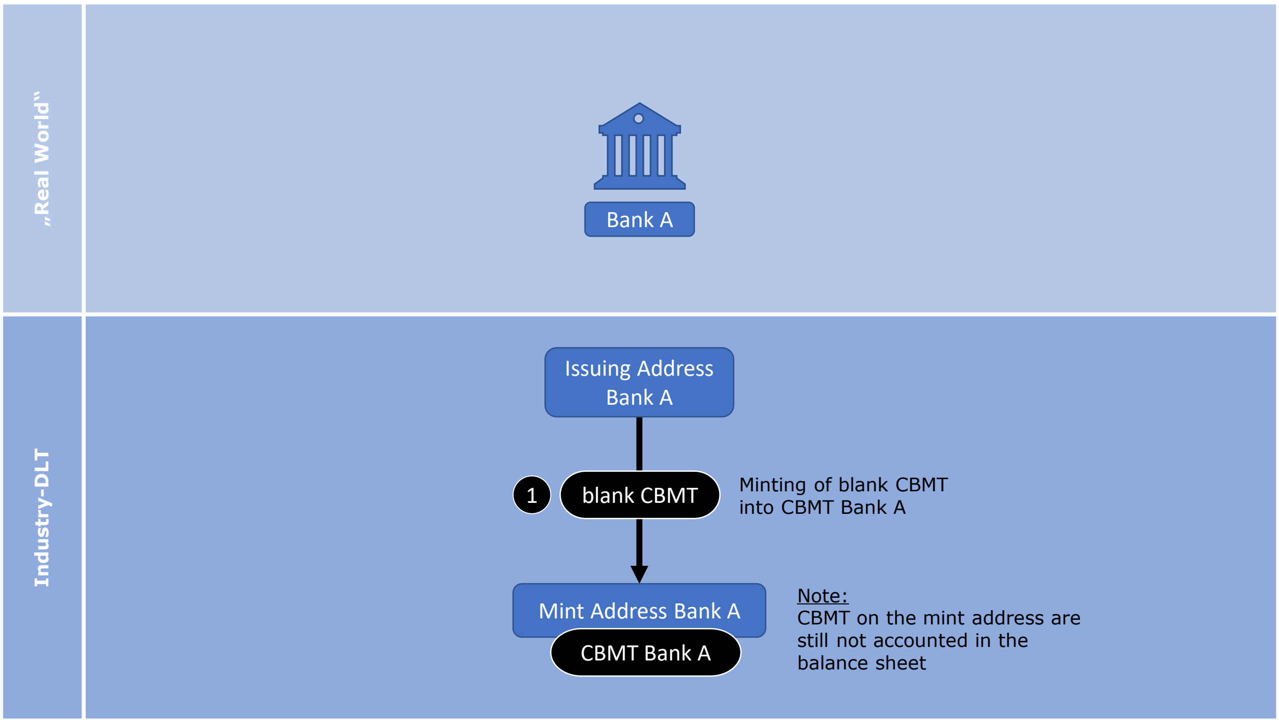


Figure 3: Mining of blank tokens

5.5.4 Minting of blank tokens into minted tokens

Thereafter, Bank A takes the blank tokens and mints them into Bank-A CBMT (metaphorically speaking, the bank stamps the tokens with a Bank-A label) and transfers them to the bank's mint address. At this point, the token already has its nominal value, but is not yet accounted in the balance sheet. This happens in the next step when the token is transferred from the mint address to the customer. After the minting process the token has a nominal value but is not recognized in the balance sheet.



Minting of blank CBMT into CBMT Bank A

Note:
CBMT on the mint address are still not accounted in the balance sheet

Figure 4: Minting of blank tokens into minted tokens

5.5.5 Converting commercial bank money into tokenized commercial bank money

The process of converting commercial bank money into tokenized commercial bank money is kind of extension of the mining and minting process described earlier. In this case the process starts with the demand of the customer to convert commercial bank money into CBMT. Therefore, the customer instructs its bank to deliver CBMT. This in turn starts the bank's internal processes of mining (via TSP instruction) and minting CBMT (explained in the two sections above). Finally, the bank transfers the minted CBMT from the mint address to the customer's general address. Once the tokens reach the customer's address, the bank accounts the tokens into its balance sheet.

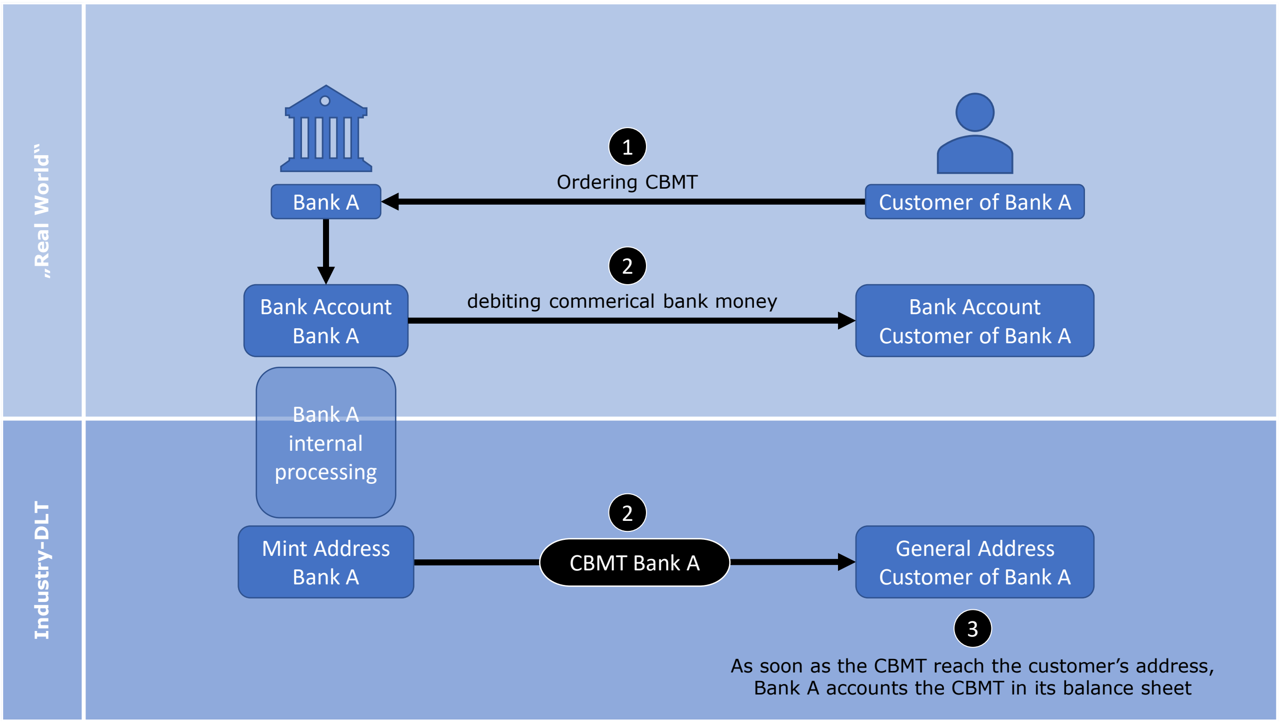

„Real World"
Industry-DLT
1
Ordering CBMT
Bank A
Customer of Bank A
2
debiting commerical bank money
Bank Account Bank A
Bank Account Customer of Bank A
Bank A internal processing
2
Mint Address Bank A
CBMT Bank A
General Address Customer of Bank A
3
As soon as the CBMT reach the customer's address, Bank A accounts the CBMT in its balance sheet

Figure 5: Converting commercial bank money into tokenized commercial bank money

5.5.6 Transfer of CBMT between customers or convert CBMT into CBM

In this case customer A wants to convert tokens of its house bank into commercial bank money. The bank accepts the Bank A tokens on its general address and credits the Bank account of customer A. The bank can decide whether to de-mint or to store the token on its general address. The de-minted token will be stored in the issuing address where the tokens can be used for a new minting. If the customer wants to convert a token from another bank into commercial bank money, that token must be exchanged for a token issued by Bank A first.

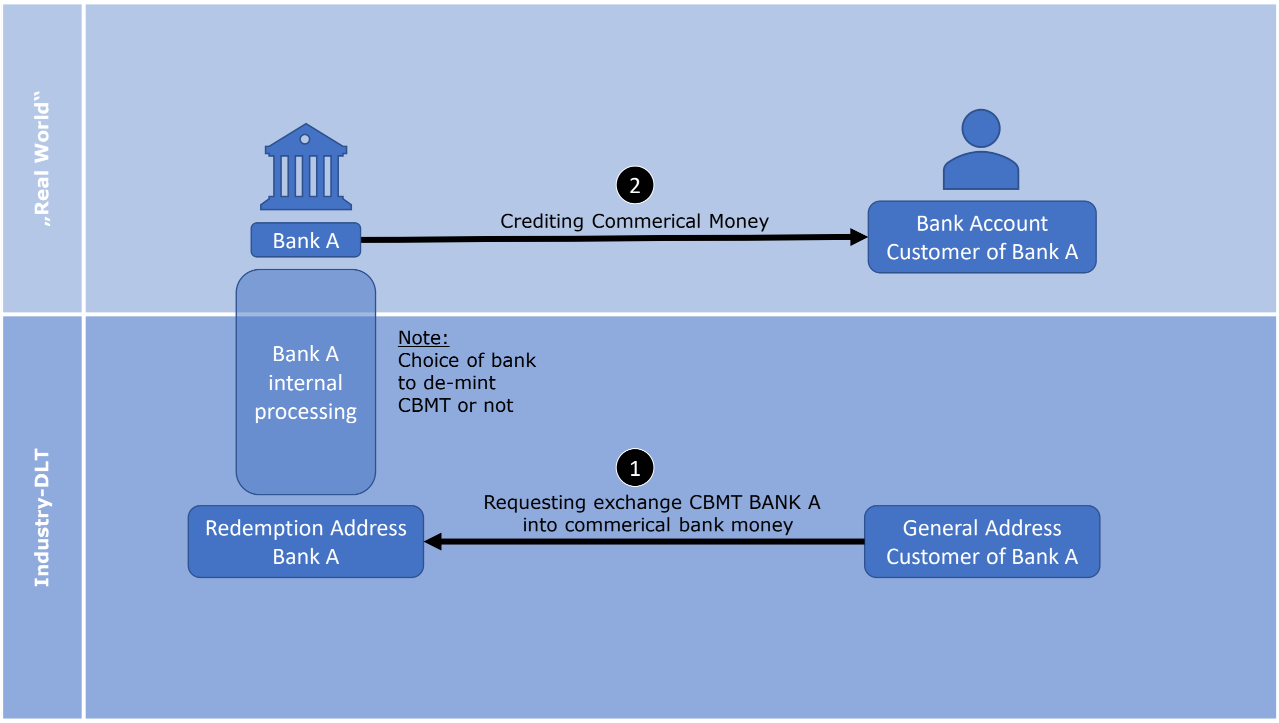

„Real World"
Industry-DLT
Bank A
2
Crediting Commerical Money
Bank Account Customer of Bank A
Bank A internal processing
Note:
Choice of bank to de-mint CBMT or not
1
Requesting exchange CBMT BANK A into commerical bank money
Redemption Address Bank A
General Address Customer of Bank A

Figure 6: Transfer of CBMT between customers or convert tokenized commercial bank money into commercial bank money

5.5.7 Transfer of CBMT between customers of different banks

The customer can only convert tokens of its house bank into commercial bank money. Hence, there is a certain interest of the customer in only holding tokens of its house bank. However, it cannot be ruled out that the customer also wants to hold tokens of another bank. Thus, we distinguish between two ways of dealing with CMBT received from another bank:
1) converting the foreign CBMT into inhouse CBMT, or
2) holding foreign CBMT.

For these two different ways of handling CBMT, each customer will have at least two addresses:

- Convert address – This is the address that the customer usually communicates to other participants for receiving tokens.
  - This address can receive CBMT issued by a bank that is associated with the general address. These tokens will be immediately moved to the general address.
  - It can also receive foreign CBMT, whereby foreign tokens will automatically be converted into CBMT of the preferred Bank. These converted tokens will be immediately moved to the general address.
- General address – tokens from another bank – If there is an explicit wish to hold foreign CBMT, the customer can communicate the general address to other participants. CBMTs sent to this address will not be converted.

These two ways of dealing with CMBT received from another bank are described in the following in more detail.

5.5.7.1 Transfer of CBMT (Converting foreign CBMTs into inhouse CBMTs)

When receiving foreign CBMTs on the convert address, the house bank will automatically convert the foreign CBMTs into CBMTs of the house bank. In this case the convert address of customer A is not associated with Bank B.

Example:
A customer of Bank B transfers Bank B CBMTs to the convert address of a customer at Bank A. Bank A accepts the foreign tokens on the customers convert address and transfers them to its general address (general bank address of Bank A). At the same time, it credits the customer the same number of inhouse tokens issued by Bank A on the customer's general address.

If there are not enough inhouse CBMTs, Bank A must mint more tokens. This presumes that Bank A either:
1) has the required number of blank tokens, or
2) need to send a request to the TSP for mining the number of blank tokens.

Note:
The payee always must specify if it wants to receive CMBT on its convert or rather its general address. Therefore, the process of exchanging into inhouse tokens takes place in the background.

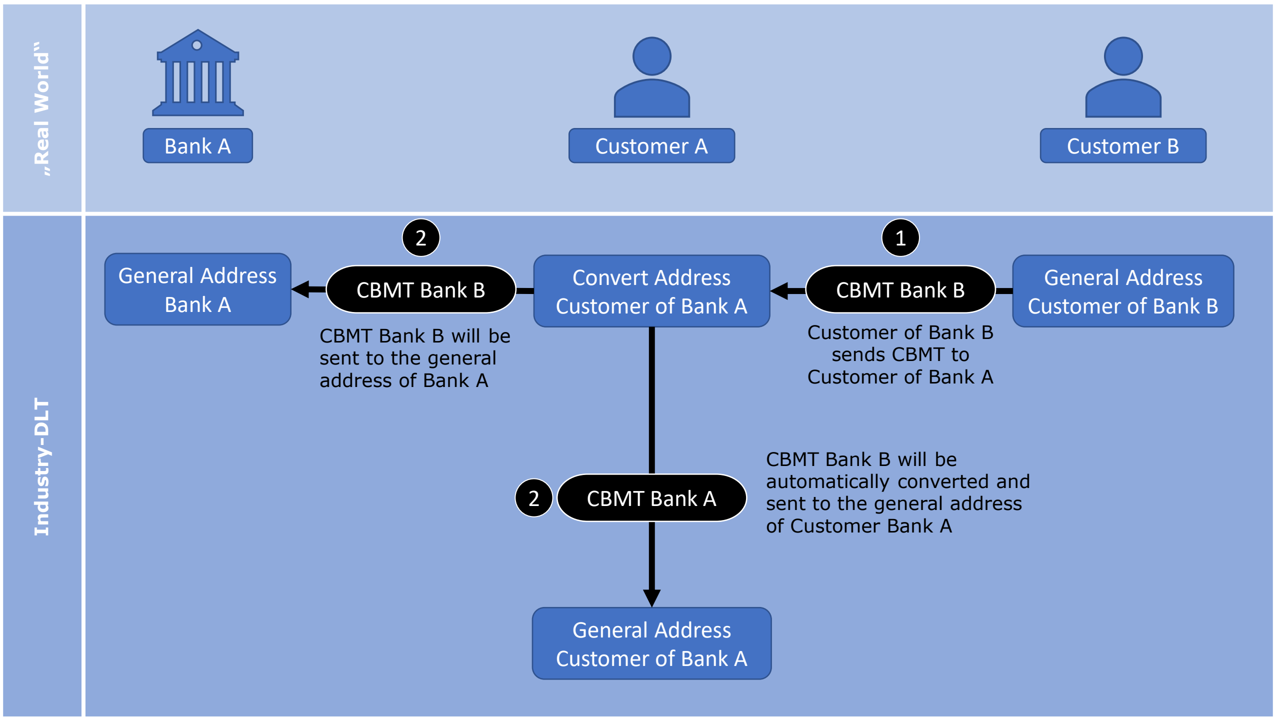

„Real World"
Bank A
Customer A
Customer B
Industry-DLT
2
1
General Address Bank A
CBMT Bank B
Convert Address Customer of Bank A
CBMT Bank B
General Address Customer of Bank B
CBMT Bank B will be sent to the general address of Bank A
Customer of Bank B sends CBMT to Customer of Bank A
2
CBMT Bank A
CBMT Bank B will be automatically converted and sent to the general address of Customer Bank A
General Address Customer of Bank A

Figure 7: Transfer of CBMT (Converting foreign CBMTs into inhouse CBMTs)

The process in the background between the banks is even more complex, because if, for example customer A sends Bank A CBMTs to customer B, these tokens are still Bank A CBMT. The original "minter" (Bank A) gave it the value. Therefore, it must be cleared or accounted between the banks (the settlement will be explained in more detail in 5.6).

5.5.7.2 Transfer of CBMT (Holding CBMTs of associated banks)

A customer of Bank B transfers Bank B CBMTs to the convert address of customer A. The convert address is associated with Bank A and Bank B. Since the convert address is also associated with Bank B, no conversion is necessary and the CBMT is moved directly to the general address of customer A.

The customer can receive and hold different tokens in his/her general address. In this case, the customer must be aware of the different CBMT types. We expect that only corporate customers or large customers desire to hold CBMT of multiple banks in order to diversify the counterparty risk.

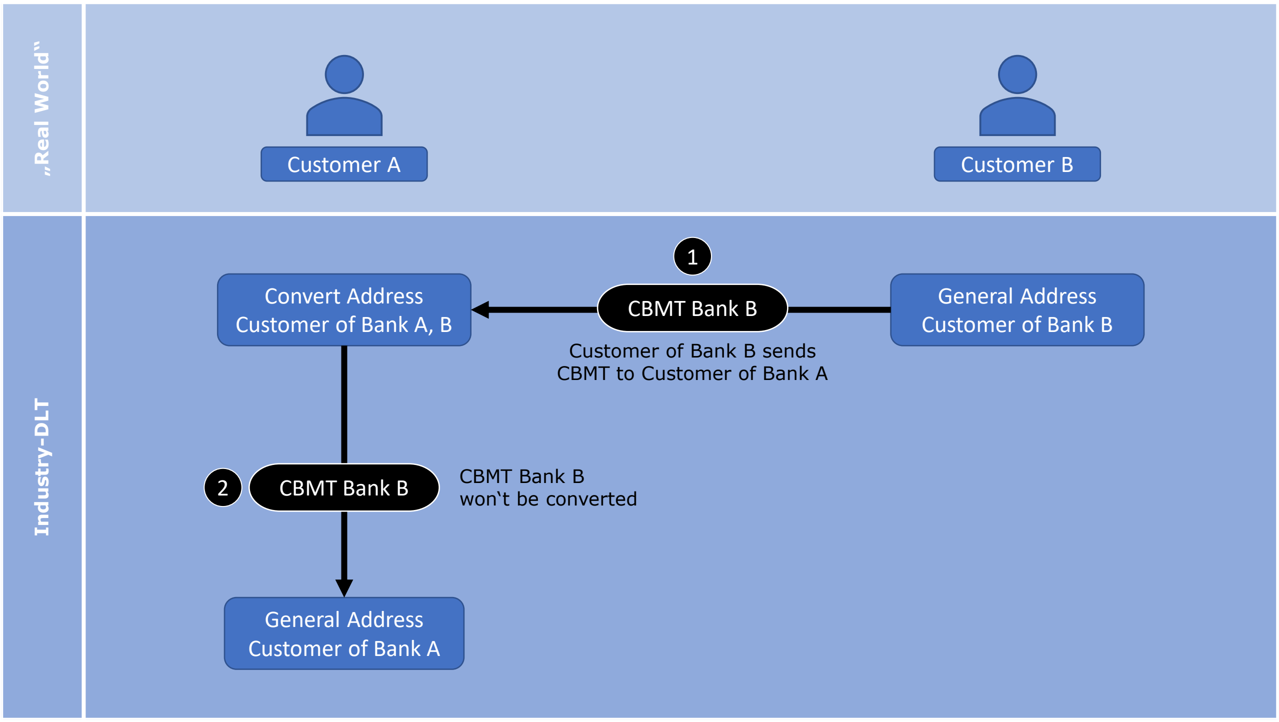
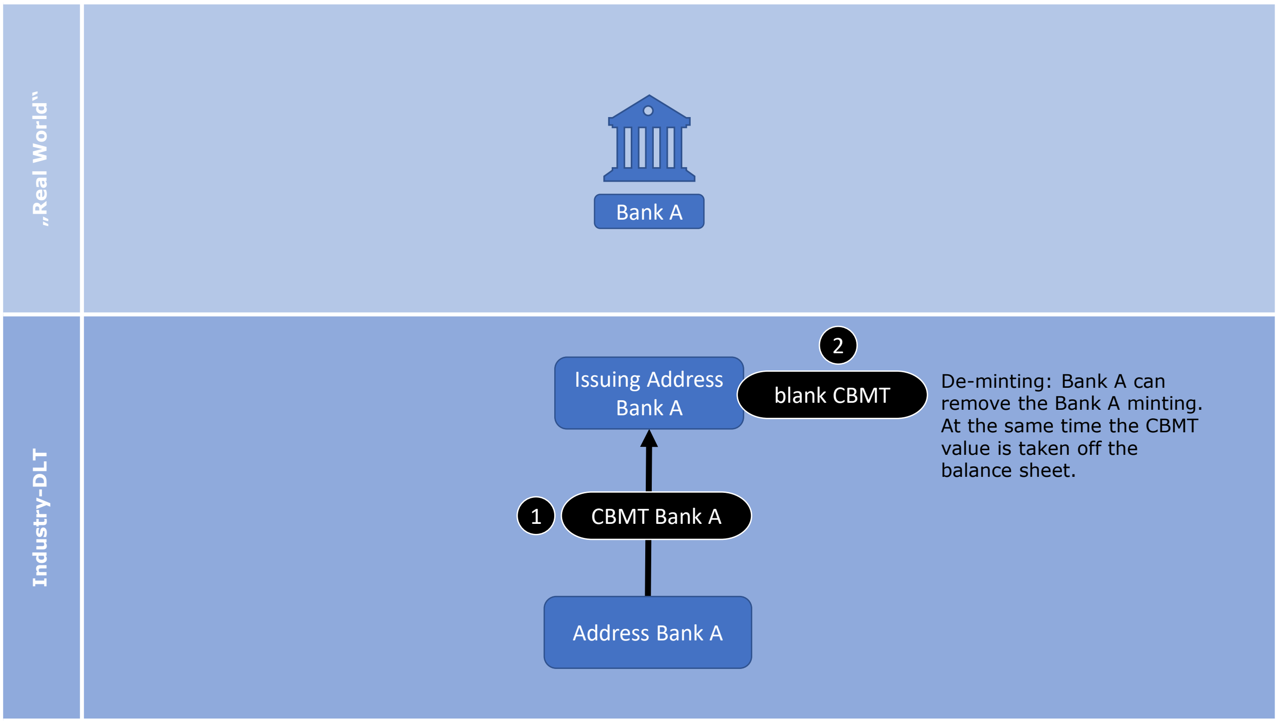

„Real World"
Customer A
Customer B
Industry-DLT
1
Convert Address Customer of Bank A, B
CBMT Bank B
General Address Customer of Bank B
Customer of Bank B sends CBMT to Customer of Bank A
2
CBMT Bank B
CBMT Bank B won't be converted
General Address Customer of Bank A

Figure 8: Transfer of CBMT (Holding CBMTs of associated banks)

5.5.8 De-minting of CBMT

When a CBMT is de-minted, the “stamp” of the issuing bank is removed. The blank / value free (worthless) token is then deposited at the issuing address. Blank tokens can be returned to the TSP from the issuing address. The stamp removal can only be initiated by the issuing bank.

The return of blank / value free tokens reduces the potential systemic risk and is desirable.



De-minting: Bank A can remove the Bank A minting. At the same time the CBMT value is taken off the balance sheet.

Figure 9: De-minting of CBMT

5.5.9 Burning of blank tokens

To remove blank tokens from the system, the TSP can burn tokens. This process is initiated by the issuing bank by submitting blank tokens from its issuing address to the TSP for burning. As the blank tokens have no value to the bank submitting the tokens, this has no effect on the balance sheet of the bank.

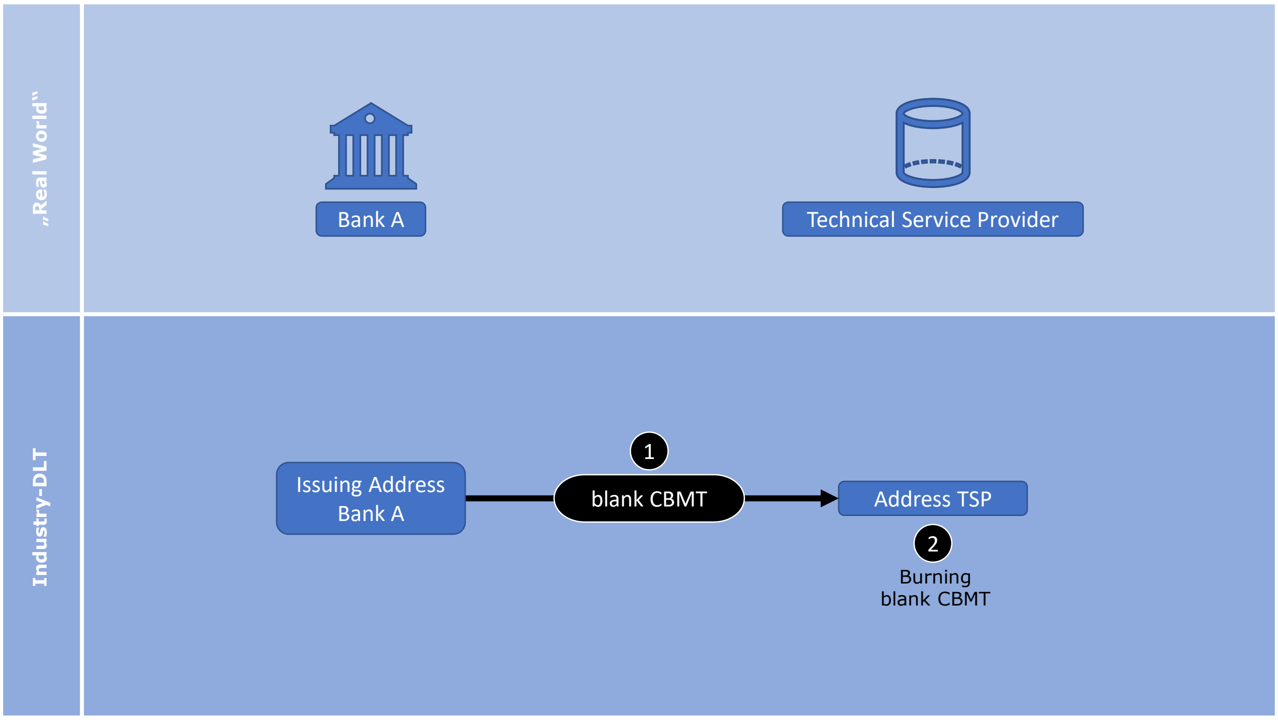


Figure 10: Burning of blank tokens

5.6 Interbank Settlement

We assume that the settlement process will evolve as the system evolves. Settlement between banks potentially includes a settlement of the difference in €. After the Settlement the banks can de-mint and burn the tokens, but do not need to. The following examples show possible approaches for settling the liabilities between two banks:

Bilateral gross settlement between two banks on a single DLT

The settlement can be initiated by the bank holding tokens against the issuing bank. Through a trigger solution, the holding bank transfers its tokens to the redemption address of the tokens and in return receives € corresponding to the token value. This process can be repeated until a bank holds no foreign tokens.

Example:
Bank A owns 100 B-tokens, 70 € Cash
Bank B owns 50 A-tokens, 110 € Cash

1) Bank A initiates the gross settlement
2) The gross settlement transfers 100 B-tokens to the redemption address of Bank B.
3) Bank B simultaneously transfers 100 € to Bank A using the traditional payment infrastructure. A trigger solution communicates the transfer to the DLT to complete the transaction.

4) Bank B adjusts its balance sheet for the received tokens.

Result:
Bank A owns 0 B-tokens, 170 € Cash
Bank B owns 50 A-tokens, 10 € Cash

Sequential net settlement between two banks on a single DLT (Alternative 1)

The bank with the smallest token amounts kicks off the settling in tokens. Either of the two banks can initiate the settlement. Through a smart contract, the same amounts of tokens can be atomically swapped between two banks. The banks only swap either tokens against tokens or tokens against €. If a bank does not have enough tokens issued by the other bank to swap, the difference is settled in € through the traditional payment infrastructure like in the case of bilateral gross settlement.

Example:
Bank A owns 100 B-tokens, 70 €
Bank B owns 50 A-tokens, 110 €

1) Bank A initiates the net settlement with 100 B-tokens.
2) Bank B rejects the settlement, as it only has 50 A-tokens.
3) Bank B initiates the net settlement with 50 A-tokens.
4) Bank A agrees to the settlement in tokens and the banks swap 50 tokens. Each bank receives the tokens on its respective redemptions address.
5) Bank B adjusts its balance sheet for the received tokens. Bank A adjusts its balance sheet for the received tokens.
6) Bank A initiates the settlement for its remaining 50 B-tokens.
7) Bank B transfers € 50 to Bank A using the traditional payment infrastructure. Bank A transfers 50 Bank B Tokens to the redemption address of Bank B.
8) A trigger solution communicates the transfer to the DLT to complete the transaction.
9) Bank B adjusts its balance sheet for the received tokens.

Result:
Bank A owns 0 B-tokens, 120 € Cash
Bank B owns 0 A-tokens, 60 € Cash

Bilateral simultaneous net-settlement between two banks on a single DLT (Alternative 2)

Either of the two banks can initiate the settlement. Through a smart contract, same amounts of tokens can be atomically swapped between two banks. If a bank does not have enough tokens issued by the other bank to swap, the difference is settled in € through the traditional payment infrastructure like in the case of bilateral gross-settlement.

Example:
Bank A owns 100 B-tokens, 70 € Cash
Bank B owns 50 A-tokens, 110 € Cash

1) Bank A initiates the net settlement with 100 B-tokens
2) The net settlement transfers 100 B-tokens to the redemption address of Bank B.
3) Bank B simultaneously transfers 50 A-tokens to the redemption address of Bank A and 50 € to Bank A using the traditional payment infrastructure. A trigger solution communicates the transfer to the DLT to complete the transaction.
4) Bank B adjusts its balance sheet for the received tokens. Bank A adjusts its balance sheet for the received tokens.

Result:
Bank A owns 0 B-tokens, 120 € Cash
Bank B owns 0 A-tokens, 60€ Cash

Bilateral net-settlement between two banks across multiple DLTs

Building on the previous examples, the settlement process can be extended to cover multiple DLTs at the same time. This reduces the number of €-transactions at the cost of higher complexity between the different DLTs. There need to be cross-chain trigger solutions to allow for coordinated swapping of assets across the DLTs.

Example:
The banks hold the following tokens across DLTs:

	DLT-1	DLT-2	DLT-3	DLT-4	€
Bank A	B-100	B-650	B-250	B-0	500 €
Bank B	A-150	A-600	A-0	A-350	700 €

In total, Bank A owns 1000 B-tokens across the DLTs, B owns 1100 A-tokens across the DLTs.

1) The bilateral cross-chain settlement is started by (e.g.)alphabetically first Bank A for an amount of 1000. Each bank reports to the other tokens (or €) to settle the amount.
2) The following transactions are executed on the various DLTs, held together by a trigger solution:
   Bank A transfers 100 B-tokens on DLT 1 to B
   Bank A transfers 650 B-tokens on DLT 2 to B
   Bank A transfers 250 B-tokens on DLT 3 to B
   Bank B transfers 150 A-tokens on DLT 1 to A
   Bank B transfers 600 A-tokens on DLT 2 to A
   Bank B transfers 250 A-tokens on DLT 4 to A
   This leaves A with 0 B-tokens and B with 100 A-tokens.
3) Bank A adjusts its balance sheet. Bank B adjusts its balance sheet.

Result:

	DLT-1	DLT-2	DLT-3	DLT-4	€
Bank A	0	0	0	0	500 €
Bank B	0	0	0	A-100	700 €

The remaining difference can then be settled using the approaches explained above.

Comparison of the different settlement approaches

The bilateral single-chain gross settlement has the smallest complexity but involves up to two € payments for each pair of banks and each DLT. The bilateral single-chain net settlement has at most one € payment for each pair of banks and DLT but up to two on-chain token transfers for each DLT. The bilateral cross-chain net settlement has a single € payment for each pair of banks and up to two transactions for each DLT but carries the most complexity in coordinating trigger solutions across DLTs.

Rejected ideas

Settlement without an atomic transaction across all DLTs. Bank A burns tokens of Bank B and debits the current account of Bank B with Bank A. This contradicts to the idea that only the issuing bank can burn its tokens. It also removes the benefit of using a DLT for ensuring atomicity when swapping assets.

5.7 Open Questions

5.7.1 Software upgrades

How will software upgrades be handled with respect to old versions of tokens? Most likely, the same process as with existing DLTs can be applied, but this needs more scrutiny.
A fallback solution is to convert old versions of tokens into fiat money which in turn is converted into new tokens.

5.7.2 Prevention of token transfers from/to non-whitelisted addresses

This scenario is not desired, but since it cannot be ruled out, possibilities and solutions must be considered. This scenario should be prevented by the restriction of token transfers to the smart contract that checks the whitelist.

The transfer API needs to list at least four elements: Amount, Issuer, Payer, Payee. An API for checking whether a transfer is from/to a whitelisted address will be a bottleneck/single point of failure. Ideally, such a check can be done without an oracle. An ex-post check can uncover such transactions later.

A smart contract could be used that only allows a customer the transfer of tokens issued by a bank from addresses assigned to the bank. This would ensure that all sender addresses for tokens are whitelisted. For customers holding tokens of multiple issuers in their address, such a contract could not be used.

Another approach would be to record the history of transfer addresses with each amount. This allows to quickly check whether all involved addresses in a transaction and its history are whitelisted. A drawback is that amounts of CBMT from the same bank cannot be merged anymore, as one needs to also consider the addresses involved in the history of each amount to be merged. For relatively short/closed money cycles with trusted addresses like a company with subsidiaries, this can still allow transactions without needing to involve the TSP or an external whitelist check.

5.7.3 Combine Mining and Minting step

The separation of Mining and Minting seems to complicate more than it simplifies. Technically the two steps can be combined into one step. Can the two steps be combined into a single step while still maintaining a clear picture on the balance sheet?

6. Supporting multiple Currencies

The following chapter describes the necessary extensions for the ability of the token to represent commercial bank money in different Fiat currencies. This is a high-level discussion to convey the general ideas, some details need to be specified.

From a technical point of view, the CBMT can represent a claim in any Fiat currency. The explicit exchange of tokens of different currencies is obvious: A customer sends tokens in currency A to his bank with the order to receive a corresponding amount in currency B. Even if only one currency is used, an implicit exchange of tokens already takes place in CBMT, since a customer can only hold tokens from a bank with which an account relationship exists. As the procedure of an implicit conversion must already be implemented for a DLT with only one currency, it seems reasonable to extend the implicit exchange process to the exchange of currencies as well.

6.1 Prerequisites

To facilitate reading and discussion, we assume in the following part that one of the banks is a EUR related bank and the customer is from a EUR country and that his base currency, i.e., with which he mainly trades, is also EUR. Of course, the following guidelines also apply even if the currency is different.

This chapter describes the technical conversion of a CBMT of a currency into a CBMT of another currency. The actual FX conversion (e. g. swapping a liability denominated in USD with a liability denominated in EUR) will be carried out based on prevailing market conditions by each bank individually similar to existing processes.

Which currencies are used on a DLT should primarily be based on the needs of the business partners using the DLT. Since the CBMT is intended to be universally usable, we cannot assume any restrictions regarding the currencies used on a DLT.

This poses two possible problems:

a) Some participating banks do not accept every currency on a given industry DLT.

b) A customer can only receive or hold tokens in a currency for which an account relationship exists with a bank. Even if a customer's bank can handle all currencies in use, the customer may choose not to have an account for all currencies in use on the DLT.

We will discuss different ways of dealing with these two situations below and state the preferred option.

6.2 Transferring a token with arbitrary currency between customers of arbitrary banks

In the following examples, we will always assume that the customer instructs business partners to send CBMT to its convert address. Receiving CBMT at the general address raises issues which are discussed in chapter 6.4.1.

Different conversions cause different costs to the customer. The goal is to choose the optimal cost for the customer. Swapping a CBMT against a CBMT of another issuer in the same currency is a mere technical process. Whereas swapping a CBMT of a certain currency against a CBMT in a different currency induces a FX market operation with the known costs (market prices, bid-offer gap etc.). Therefore, we assume that a currency conversion is more costly than changing the issuer of the token. The costliest conversion must take place when issuer and currency must be changed.

Depending on whether the customer can receive the currency sent and which banks are registered with the receiving address, four different cases are possible:

		Address registered with the issuer bank	
		Yes	No
Customer can receive token currency on convert address	Yes	No conversion (1)	Issuer needs to be changed, currency remains the same (2)
	No	Currency needs to be changed, issuer remains the same (3)	Issuer needs to be changed, currency needs to be changed (4)

The above table implies an algorithm for determining the conversion cases. This algorithm is illustrated explicitly by the following flow chart.

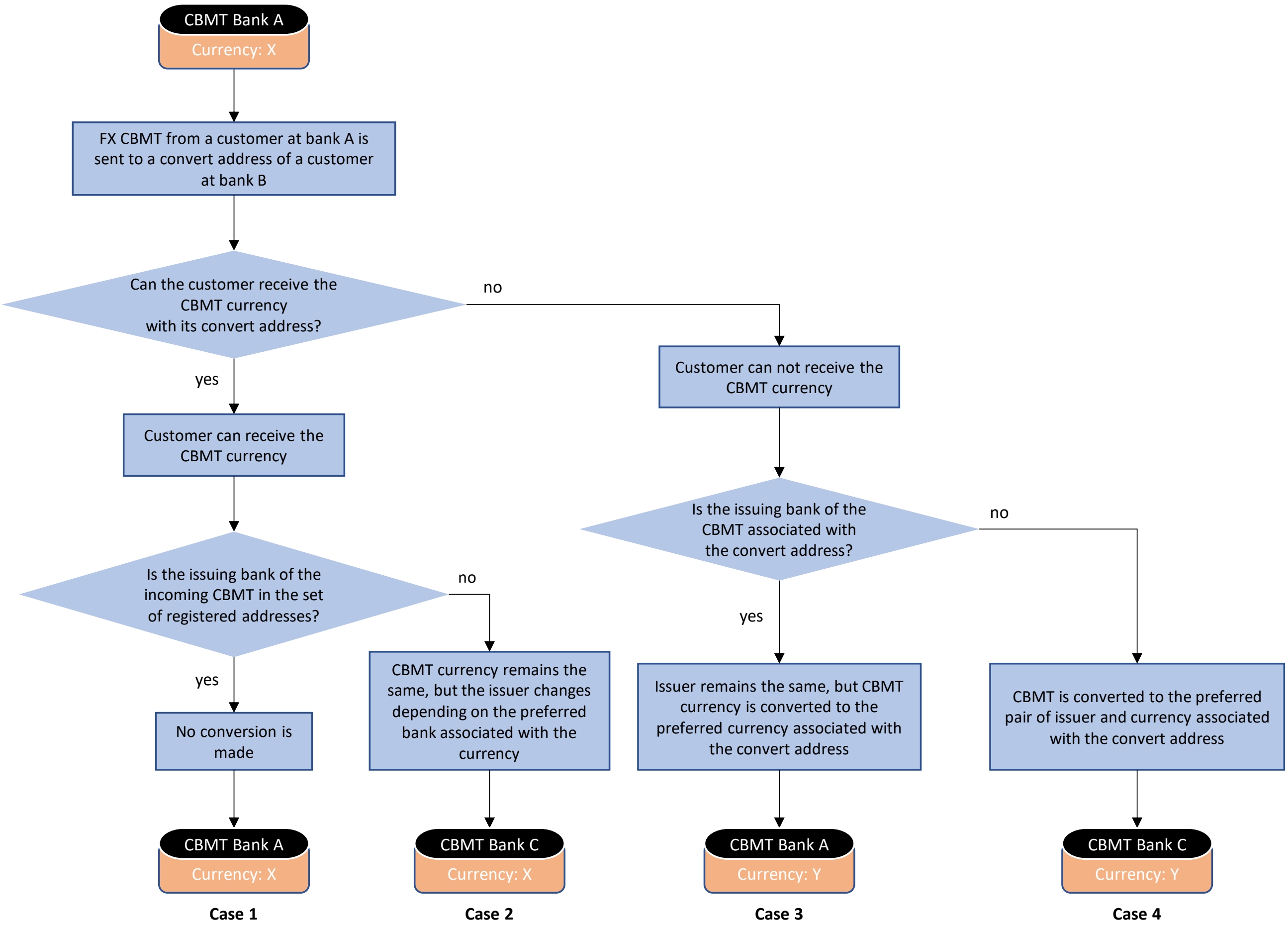

CBMT Bank A
Currency: X
FX CBMT from a customer at bank A is sent to a convert address of a customer at bank B
Can the customer receive the CBMT currency with its convert address?
no
yes
Customer can receive the CBMT currency
Customer can not receive the CBMT currency
Is the issuing bank of the incoming CBMT in the set of registered addresses?
no
yes
Is the issuing bank of the CBMT associated with the convert address?
no
yes
No conversion is made
CBMT currency remains the same, but the issuer changes depending on the preferred bank associated with the currency
Issuer remains the same, but CBMT currency is converted to the preferred currency associated with the convert address
CBMT is converted to the preferred pair of issuer and currency associated with the convert address
CBMT Bank A
Currency: X
Case 1
CBMT Bank C
Currency: X
Case 2
CBMT Bank A
Currency: Y
Case 3
CBMT Bank C
Currency: Y
Case 4

Figure 11: Flow chart of token conversion algorithm (multi currency)

6.3 Considerations regarding banks

There are different approaches to how banks will treat different currencies on a DLT. We discuss the alternatives and propose a way forward.

6.3.1 All banks accept a fixed set of currencies

All participating banks agree ex ante on a fixed set of currencies that will be supported by the CBMT for a given DLT. This must be agreed in advance and contractually secured before a bank is involved.

This implies that payments in all agreed currencies are accepted by all banks. This seems like the cleanest method to solve the problem.
On the downside it raises the entry bar for banks to participate. Furthermore, this also leads to a certain inflexibility when the need for supported currencies on a DLT changes, since all banks needs to agree changing the set of supported currencies.

6.3.2 Banks with different accepted currencies

If the banks do not agree on a common set of currencies, it is possible that it is attempted to send a token to a bank with a currency that is not accepted by the bank. This must never happen.

Therefore, the smart contract must have the information which banks accept which currencies. In case the currency of the CBMT is not supported by the receiving bank, the smart contract rejects to move the CBMT. From a customer's perspective, such a rejection is clearly undesired.

6.3.3 Exchange handled by a Sponsor

Each currency pair (X, Y) on a DLT must have a "designated sponsor". A designated sponsor is a bank which must accept the request of another bank to exchange a CBMT of currency X in CBMT of currency Y or vice versa.

All banks which do not natively support a currency pair must use a designated sponsor to perform the currency conversion which they do not natively support. The result is that all banks can accept any currency pair for payment. Since this is the best alternative for the customers, it is the preferred option. To keep it simple for the banks, a standard smart contract will be made available to banks for the currency exchange. Governance around the sponsor has been left out deliberately and will be discussed going forward/separately. We expect the sponsor to be one of the participating banks, but this is not mandatory. The mechanism to ensure that there is always a sponsor available is described in 7.8.

If the sponsor needs to make a currency exchange, the sponsor takes the tokens from the sending bank, and issues its own tokens with the target currency according to the (agreed) exchange rate. These tokens are sent to the target bank.

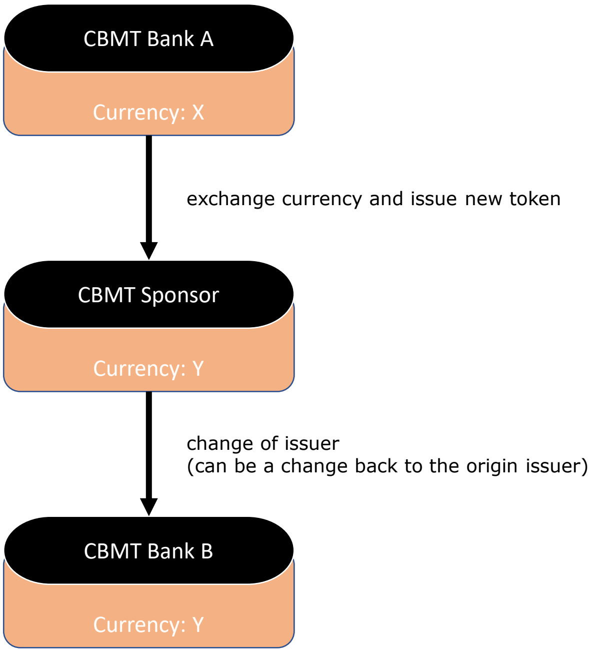


Figure 12: Exchange handled by a Sponsor

6.4 Considerations regarding customers

Customers may consider automatic currency conversion as an appreciated service, freeing them from the need to have a plethora of FX accounts and eliminating FX risk.
The set of currencies accepted by a customer is determined by the set of current accounts with its banks. The bank activates the possible currencies for the customer on the convert address. To enable automatic FX conversion, for each convert address a preferred currency must be specified. Other currencies which are not accepted shall be converted into that currency. If the customer receives token of a currency that is not specified at his convert address, the token will always be converted to the preferred currency.

6.4.1 Considerations for convert addresses

The following three configurations are mandatory:

1. Preferred issuer per currency. To handle conversion cases 1 and 2, for every preferred currency exactly one preferred issuer has to be defined. This is the issuer of the token that will be transferred to the general address.
2. Preferred issuer per convert address. To find an issuer when a currency is not associated with any of the issuers associated with the convert address (case 4).
3. Preferred currency. All CBMT in currencies the customer is not able to store in his general address will get converted into the preferred currency (cases 3 and 4). For the CBMT in the preferred currency, the issuer must be defined.
   There is only one preferred currency per convert address. If the customer, for example, always

wants an automated change from Mexican Peso to Euro he must use another convert address then when he wants to do an automated change from British Pound to US Dollar.

6.4.2 General address as receiver address

In the previous chapter we assumed that we always use the convert address as receiver address. However, if the customer explicitly wants to use the general address as receiving address, the 4 cases will be handled the following way:

- Use case 1 (no conversion) is obviously supported.
- For the other uses cases 2, 3 and 4, there are two alternative approaches:
    1. Reject the transaction. The (sending) party gets informed that the transaction failed, like with other cases, e. g. no funding.
    2. Redirect the CBMT to the convert address. Since the customer is allowed to have multiple general addresses and multiple convert addresses, the customer would need to specify a complete mapping between general and convert addresses.

We prefer approach 1, because approach 2 seems counterintuitive: The standard process is to move CBMT to a convert address. If the customer intentionally deviates from the standard process, it makes no sense to automatically enforce the standard process. Furthermore, approach 2 adds complexity outweighing the potential benefits.

6.5 Further considerations

6.5.1 Deposit insurance of foreign currency

By law (EinSiG), all accounts in any currency are included in the calculation. The currency conversion happens according to the ECB daily rate. In this respect it can be assumed that the same applies to tokens in foreign currency.

7. Sketches for „unhappy events" with CBMT

These sketches outline possible approaches to events during the CBMT lifecycle. Most of the interesting problems occur whenever tokens are locked outside of whitelisted addresses, for example in escrow for Smart Contracts. Whether this problem is out of scope for CBMT remains to be seen. The solutions for locked tokens are similar to the existing solutions in existing DLTs.

7.1 Single bank leaves a DLT (DLT not used anymore)

Leaving a single DLT is an important step if the DLT is not used anymore, and the traffic does not justify the costs. The following steps allow a bank to leave a DLT unilaterally:

1) Stop converting commercial bank money into new tokens.

2) Convert all tokens held by direct customers into commercial bank money.
3) Initiate €-settlement with other banks still holding tokens issued by this bank.
4) Initiate €-settlement for all tokens still held by the leaving bank.
5) De-mint and burn all tokens issued by the leaving bank.

Since all valid tokens must be held with a participating bank, the case of tokens held by a non-bank in self-custody cannot happen. Any such outstanding tokens must be settled by the non-bank outside of the DLT. Tokens held in escrow will remain locked in escrow. Potentially the token substitution mechanism can be used to replace these tokens by tokens of other banks (with which the customer has a relationship). If there are other banks, the leaving bank can arrange a conversion of its tokens into tokens of a remaining bank or prearrange an €-settlement with the remaining banks. If no other banks remain on the DLT, the tokens held in escrow must have been issued by the leaving bank. If possible, the bank must resolve the escrow relations and instate corresponding escrow accounts in € to be used to pay the customers.

7.2 Immediate shutdown of all CBMT on a given DLT

In the case of a hack, a software malfunction or regulatory decision, it can become necessary to cease all operations on a DLT immediately. In this case, the following process allows a graceful shutdown:

- The TSP declares the shutdown of all CMBT on a given DLT at a given timestamp. The governance structure for the TSP is still to be discussed.
- Stop converting commercial bank money into new tokens.
- Convert all tokens held by direct customers at the checkpoint timestamp into commercial bank money. If this is not possible on the DLT anymore, the tokens must be revalued to zero.
- Settle the € differences between banks according to the holdings at the timestamp. If this is not possible on the DLT anymore, the tokens must be revalued to zero / de-minted
- Customer processes in progress while the CBMT shutdown is active are problematic (locked tokens)
- Payments / transfers after the checkpoint timestamp need to be resolved outside the DLT using the legal framework

This process requires a way to later unlock tokens held in escrow by manufacturing processes. Potentially, customers will want to replace tokens held in escrow on one DLT with equivalent tokens in escrow on a different DLT while keeping the transaction on the DLT in shutdown.

7.3 Default / Moratorium of a participating bank

The deposit insurance mechanism for consumer accounts does not necessarily apply to CBMT. The address risk needs to be managed. Additionally, the case of badly programmed smart contracts being stuck needs to be considered. Smart contracts can get stuck when the tokens they hold cannot be transferred anymore or when they wait for a condition on tokens to be released and that condition cannot happen anymore since the tokens are not fungible anymore.

In the case of a default / moratorium of a bank, the following things happen:
No other bank accepts tokens of the defaulted bank anymore. This means that all automated processes holding defaulted tokens in escrow get blocked and cannot successfully complete. A rollback of such processes should be done wherever possible, but a reversal is not always possible if for example the production of physical items has already started. The defaulted tokens held by other banks are not allowed to be transferred to non-banks anymore to prevent their usage in badly programmed automated processes that don't know about the default. All defaulted tokens represent unpaid receivables against the defaulted bank.

The addresses that belong to the defaulted bank must be excluded from the whitelist (see chapter 5.2)

- **Approach 1: banks create a deposit insurance fund for CBMT**
  - A potential way around this could be to instate additional deposit insurance borne by all participating institutes. This insurance could then be used to make good all customers impacted by the default and keep all processes requiring CBM tokens issued by the defaulted bank. In this case, the default could be handled just like any single bank leaving a DLT.

- **Approach 2: CBMT has no deposit insurance**
  - The tokens issued by the defaulted bank have no value anymore. The tokens cannot be transferred anymore. All holders of such tokens experience a 100% loss. A solution for long lasting smart contracts needs to be evaluated.

- **Processual solution**: While defaulting tokens are a problem, all processes and Smart Contracts written by customers should have a provision to swap out tokens held in escrow against other tokens from a different issuer. Potentially, use of this function could be restricted to the TSP to be only used in the case of a default. This approach ensures that in case of a bank's default, the processes can continue if the customers have other tokens to restore the liquidity. This approach does not help the customers left holding the bag of defaulted tokens.

7.4 Customer leaves the DLT

Due to regulatory action or of their own decision, a customer might leave the DLT unexpectedly. In both cases, the addresses associated with the customer get removed from the whitelist by the bank. This means that token transfers from or to those addresses are not possible anymore if the smart contract is used that checks the whitelist. Any outstanding transactions need to be settled outside of the DLT. How the transactions in the DLT are handled is still under discussion.

Note: Depending on the circumstances, each bank can decide differently whether they remove the addresses of the customer with them from the whitelist. Each bank manages the whitelist for the addresses of their customers.

7.5 Default of a customer with money in escrow

If a customer defaults and has tokens locked up by a smart contract, there is no easy approach about how to unwind the contract or release the tokens. For example, if the tokens will only be released on condition of the release of goods and that release will never happen, the smart contract remains in a locked state. The handling of such locked-up tokens needs to be handled appropriately by the judicial system. A liquidator can potentially order such escrow to be lifted, and this judicial change must be reflected by the DLT. One solution could be to have the TSP break/revert such transactions within the DLT, but such a default usually has repercussions outside of the DLT as well.

Such a reversal needs to be done on a case-by-case basis since the legal framework for defaults is different between jurisdictions.

Again, a provision to allow tokens to be swapped out against otherwise worthless tokens just to let the software continue the other processes should be considered as an approach to fix smart contracts that do not consider this event or do not have appropriate timeouts.

7.6 Cross-DLT payment

The previous payment descriptions only describe operations within a single DLT. If customer A on DLT-1 wants to transfer money to customer C on DLT-2, a cross-DLT payment has to be arranged. The routing of such payment arrangements is outside of the scope of this document. In general a cross-DLT payment needs a bridge provider who has a presence in both of the DLTs and an API to specify the recipient on the other DLT within the mechanics of the first DLT. This approach can later be extended to a routing chain spanning multiple DLTs, but we restrict the discussion to a single payment spanning between two DLTs.

Example:
Customer A on DLT-1 wants to pay customer B on DLT-2. There exists an operator of a token bridge ("exchange office") that accepts DLT-1 tokens and a DLT-2 recipient address and transfers DLT-2 tokens to the intended recipient on DLT-2.

The bank holds the following tokens across DLTs:

	DLT-1	DLT-2
Customer A	A-100	
Bank A	100 €	
Bridge		
Bank C		
Customer C		

The following steps transfer the amount of 100 € in DLT-2 tokens to customer C:

Customer A transfers 100 A-tokens on DLT-1 to the bridge operator.

The bridge operator accepts 100 A-tokens on DLT-1 and sends 100 B-tokens to the entry address of customer C.

Bank C accepts the 100 B-tokens and credits the customer C with 100 C-tokens.

The debt situation is now as follows:

	DLT-1	DLT-2
Customer A		
Bank A	100 €	
Bridge	A-100	
Bank C		B-100
Customer C		C-100

The bridge settles the 100 A-tokens against Bank A on DLT-1, receiving 100 €.
The bridge settles the 100 € against Bank C on DLT-2, receiving 100 C-tokens.

This leaves Customer A with 0 A-tokens and Customer C with 100 C-tokens.

	DLT-1	DLT-2
Customer A		
Bank A		
Bridge		
Bank C		100 €
Customer C		C-100

Open issues:
Ensuring proper dvp across DLTs to ensure proper interlocking of processes is not addressed by a unidirectional bridge. Integration of a bridge into the business process must still be solved. It is unclear whether there is a general API or general approach to integrate this.

7.7 Limiting token transfers

We see two approaches to token transfers. One approach is a smart contract that consults the whitelist for every transfer. The second approach is to allow transfers without consulting the whitelist immediately. For this second approach recording the history of transfers is necessary. See also 4.1.

7.7.1 Tracking of token transfers

For payment transactions without the technical service provider (TSP) e.g., internal transfer (group) we need to prove that a token still has a value and is valid. For that we need a tracking of the addresses where the token was previously kept. A kind of history. This avoids the need for a request to check with the TSP for each transfer.

We only need a set of the addresses. We do not need to know if the token was kept first on address A and then on address B or on address B first. We only need to know that these two addresses kept it before. So, we will speak of a “Set of history addresses”.

This address-set can only store n entries (we think 10-20 max) and is only filled if payment transactions are made without the TSP.

Transactions can only be carried out if sender and receiver are already in the history or if there is room in the history to add the sender.

A finite look-back is not sufficient to recognize whether a token has left the system of whitelisted addresses without a request to the TSP.

To add that tracking information on the token it must be allowed that the tokens can be split into the requested amount.

To avoid having too small denominations of split tokens, it must be allowed to merge them under the following conditions:

- The history (set of addresses) is identical
- The issuer is identical

Merging can be done explicitly or implicitly.
By sending split tokens to a whitelisted address the split tokens get implicitly merged with the amount held by the address.
An explicit merge can be done by using a special smart contract provided by the TSP, which takes two split tokens and returns one merged token to the sender.

Any successful merge deletes the history.

7.7.2 Token transfers without TSP

It should be possible for a customer to send tokens to other addresses or other customers (on the same DLT) without the TSP, i.e., without verification. The verification of these addresses then takes place with the next transaction of the token, which is carried out with the TSP. It can therefore happen that the token has been sent to different addresses without any verification having taken place with the TSP. Therefore, all addresses recorded in the history must be verified with the TSP during the next TSP-powered transaction. If all addresses are whitelisted the history gets cleared. If the token was sent to at least one address that is not on the whitelist, the token loses its value.

To avoid this, the customer can ask its bank to carry out all needed regulatory checks in order to whitelist the address. After successful checking, the bank instructs the TSP to whitelist the address under consideration (before the next transaction of this token with verification).

7.8 Retreat of Designated Sponsor of a Currency from a DLT

To ensure that payments can always be accepted by a customer and to facilitate support for cross-currency payments on a DLT, a Designated Sponsor is required for every currency pair on a DLT. If such a Designated

Sponsor leaves the system or is not able to provide the FX service anymore, the DLT is left without an exchange facility. There are two possible approaches to remedy such a situation.

7.8.1 Require multiple sponsors for a currency pair

The approach of assigning the top institution by currency transactions as the new designated sponsor ensures the availability of the exchange facility. As the top 3 institutions for an FX pair are informed that they are the backup sponsors, they are contractually required to offer the facility.
During operations, the TSP will track the volume and number of currency transactions for each currency pair on a daily basis. The three institutions with the most transactions/volume for a given currency pair are backup sponsors. If the Designated Sponsor leaves the DLT, one of the backup sponsors becomes the Designated Sponsor.

7.8.2 TSP as sponsor of last resort

The TSP can offer the FX capability for any currency pair by contracting with one or more banks. This puts the TSP in the position of a market participant, which may be undesirable.

We prefer option 1 so that the TSP doesn’t perform any trading/market function.

7.9 Shutdown of a currency on a given DLT

Due to for example regulatory action, it may happen that a currency can no longer be legally traded on a given DLT. Possible approaches to handling the situation are:

7.9.1 Credit all tokens in currency to bank accounts

All tokens in the currency are credited to an account of the customer with the respective issuer in the currency. This is possible since all customers hold only tokens by an issuer, they also have a contract with. Any further handling of the currency is then left to the off-chain processes and contracts between the bank and the customer.

7.9.2 FX conversion to a new currency

Each CBMT holder of a given currency decides into which new currency the tokens should be converted. Tokens that are not converted this way get retracted from the DLT and credited to an account of the customer in the currency.
We would offer both options to our customers.

7.10 Offline Use Case

The adoption of the offline model offers the opportunity to augment the availability of services at the cost of considerable risks, usually related to the so-called “double spending problem” or the risk of counterfeiting: payments that are not verified against the payment service, cannot be checked in real time (from: A digital euro: a contribution to the discussion on technical design choices July 2021).

Despite the risk, there are some use-cases that are attractive for some customers and therefore necessary to discuss.

This Use Case needs to be examined more closely, as it could become complicated. In the first draft we will exclude it, but it should still receive attention.
At the moment, we assume that two scenarios need to be examined:

- One of the counterparts is always online, the other is always offline.
- Both are offline, one can/must go online "later".

Transactions between two offline parts that cannot go online must be prohibited.

8. Benefits of CBMT for customers

With the described approach, industry customers can benefit from the availability of CBMT in various forms:

- As issuing banks guarantee the 1:1 exchange of CBMT into commercial money at any time and unlimited, CBMT has the same inherent trust level as the well-known commercial bank money. There is no need for a separate and additional risk management by customers.
- CBMT-issuing banks support a link between CBMT and the commercial bank money, i.e., the customer can exchange both forms of money any time. This includes unlimited store of value for CBMT.
- CBMT are available directly on industry DLTs, i.e., there is no separate payment processing to be initiated. The industry chain keeps full control on financial flows at any time as integral and inherent part of the industry value chain.
- It is possible to program transactions leveraging CBMT to address industry-specific needs or leverage technological benefits of a selected DLT framework.
- The industry can select any wallet provider to support their needs.
- There is no need to respect conventional payment flows and its specific rules and regulations.

9. Proposal for Content of Product Guidelines for a CBMT

Following items should be part of product guidelines for CBMT:

1. Vision and Objectives
   - 1.1 Vision
   - 1.2 Objectives
   - 1.3 Commercial Context for Users and Providers
   - 1.4 The Business Benefits
2. Definitions
3. Features
   - 3.1 Common Legal Framework
   - 3.2 Additional Optional Services
   - 3.3 Currency
   - 3.4 Value Limits
   - 3.5 Reachability
   - 3.6 Actors
   - 3.7 Clearing and Settlement Mechanisms
4. Business and Operational Model
   - 4.1 Processing Flow
   - 4.2 Time Cycles
5. Rights and Obligations of participants
6. Liability
7. Management Rules
   - 7.1 Development and Amendment procedure
   - 7.2 Compliance
   - 7.3 Cooperation and information exchange
8. Governing law, jurisdiction and place of performance

Additional items:

- Adherence
- Event of suspension or termination
- Termination by Participant
- Extraordinary Termination
- Risk Management
- Security requirements
- Business continuity and contingency procedures
- Dispute resolution and applicable law
- Data protection, prevention of money laundering, administrative or restrictive measures and related issues
- Amendment procedure Guidelines
- Entry into force and binding nature

11. Glossary

WORD	Abbreviation	Description
ADDRESS		The address on a DLT is where the token are stored. Its like a normal account.
ANTI MONEY LAUNDERING	AML	Processes to prevent money laundering
ATOMIC SWAP		Atomic swaps enable parties on different blockchains to exchange tokens (of various kinds). Since an atomic swap is settled by means of a smart contract, there is no need for an intermediary to be involved in the token swap; nevertheless, the two parties are not subject to a risk of loss at any time. In addition, neither the recipient nor the payer has to provide or use their private key, so that atomic swaps are particularly safe. Technically speaking, the technology for many conventional cryptocurrencies is based on Hashed Timelock Contracts (HTLC) and hash functions. HTLC smart contracts ensure that the swap is either completed or not executed at all.
BEARER-INSTRUMENT		Bearer instruments are clearly identifiable, so that the holder of a bearer instrument can enforce a direct claim against the issuer. In the analogue world, cash and cheques are bearer instruments. Purely digital RTGS systems are based on a mirror account with a third party, an intermediary, and cannot be understood as a bearer instrument. A CBDC could be designed as a bearer instrument; either through "possession" of a digital object (= a token) or through the power to dispose of a private key that governs access to the digital objects. Users could execute payments merely by transferring the object with a valid signature, and without the involvement of an intermediary. If such a bearer instrument had offline capability, a CBDC of this kind could be functionally equivalent to cash or an endorsed cheque.
COMMERCIAL BANK MONEY TOKEN	CBMT	Tokenized commercial bank money is the response of private credit institutions to digital central bank money (CBDC). Commercial bank money can be used by non-banks as a digital means of payment and store of value. Tokenized commercial bank money will continue to be generated by commercial banks through lending or asset purchases or after debiting the customer's current account and can be exchanged at face value into central bank money at any time. Tokenized commercial bank money is thus expected to have the properties of today's commercial bank money. Tokenized commercial bank money can be transferred "peer-to-peer" (P2P) between persons, institutions, machines, etc. Benefits of DLT can be used in the real economy and in industry (DvP, automated and programmable transactions, faster and more cost-effective settlement, M2M payments, micropayments, etc.).
CLEARING		Trading in financial assets leads to debit and credit items. Clearing is the settling of bilateral or multilateral obligations between market participants. The term can also encompass other activities such as trade confirmation. The clearing process therefore establishes mutual receivables, payables and delivery obligations. In the governance of tokenized commercial bank

		money, clearing would take place on a blockchain, i.e., it would be final and occur in real time.
COMMERCIAL BANK MONEY	CBM	Unlike central bank money, commercial bank money (also referred to as book money or scriptural money) is created by credit institutions. It is an integral part of money supply and accepted as a means of payment, but it is not legal tender like cash. Commercial bank money is a claim against the issuing bank.
DISTRIBUTED LEDGER TECHNOLOGY	DLT	A distributed ledger is a “distributed digital analogue to the traditional bookkeeping journal” (BSI). DLT is characterized by distributed data storage in a peer-to-peer network where data updates are decided jointly by network nodes in a consensus. There is no central communication control or data storage; instead, the network nodes manage local copies of all the data and can add data themselves. A consensus mechanism ensures that the distributed data are up-to-date and consistent in all the nodes. Cryptographic procedures are used to secure network access, data structure and, where applicable, also consensus-building. The best-known DLT design is “the” blockchain, of which different forms exist. Another DLT design is IOTA’s “Tangle”, which is not a unidirectional chain but a “directed graph”. A directed graph is a series of nodes that are interlinked through paths that can only be passed in one direction (e.g., the street map of a city that only has one- way streets would be a directed graph and the crossroads would be the nodes).
FUNGIBILITY		The property of an asset that enables it to be identified and exchanged within the same category. **Fungible tokens** are homogeneous assets; for this reason, they are arbitrarily exchangeable and hence interoperable. Fungible tokens can be created by a smart contract which assigns to the token predefined and/or standardized attributes (e.g., same currency unit). If tokens are fungible, they cannot have individual properties and are therefore not programmable money. Consequently, they cannot be used for a specific purpose. However, they can easily be used as tokens in programmable payments. **Non-fungible tokens** are unique assets, such as a work of art (see CryptoKitties). If various money tokens are non-fungible, this may lead to exchange rates between the tokens and other disadvantageous economic effects. Tokenized commercial bank money should therefore be fungible, i.e., it should have the same properties regardless of the issuer and, hence, be exchangeable. Fungible commercial bank money can be exchanged 1:1 into tokenized commercial bank money of other issuers (full-service banks).
KNOW YOU CUSTOMER	KYC	Standards that are designed to protect financial institutions against fraud, corruption, money laundering and terrorist financing. KYC involves several steps to establish customer identity; understand the nature of customers’ activities and qualify that the source of funds is legitimate; and assess money laundering risks associated with customers.

MICAR		A proposal published by the EU to regulate cryptocurrencies
SETTLEMENT		Settlement fulfils obligations arising from payment and securities transactions between two or more parties with debt-discharging effect. Both central bank money and commercial bank money can be used to fulfil obligations. Settlement is usually preceded by clearing.
SMART CONTRACT		In the context of blockchains, a smart contract is usually an executable program whose execution generates a transaction on a blockchain. A smart contract can, for instance, trigger a payment once a predefined condition has been fulfilled. The term Smart Contract was introduced by Nick Szabo in 1994 for "computer-aided transaction protocols which execute contractual provisions" and it was revived with the advent of the Ethereum blockchain. Some developers of other platforms use other names and terms for executable programs on their blockchain. In the case of Hyperledger Fabric, for instance, the name used is "chain code" or, in a broader sense, "distributed applications" (dAPPs).
TECHNICAL SERVICE PROVIDER	TSP	See chapter 4
TOKEN (ECONOMIC DEFINITION)		Clearly identifiable object that represents a value and hence a store of value. A token can be seen as analogous to a clearly identifiable banknote.
TOKEN AND ACCOUNT (TECHNOLOGICAL DEFINITION)		**Token:** Representation of a defined asset on a blockchain. A token is represented by a clearly identifiable hash. The most important properties of a cryptographically strong hash are that, if only 1 bit of input data changes, the resulting hash will change significantly, and that the hash is easy to calculate based on the available data, while it is nearly impossible to derive the underlying data from the hash (referred to as "trapdoor function"). It is therefore difficult to imitate a hash, which is crucial for the integrity of payments on the blockchain. A token has the inherent properties assigned to it by the smart contract. Example: A token based on the ERC-20 standard, a fungible token. **Account:** Address by means of which information is recorded on the blockchain. Conceptually, these account addresses are comparable with conventional bank accounts. The difference compared with traditional accounts is that on the Ethereum blockchain, for instance, accounts and corresponding account balances are stored on the participating network nodes in a distributed and decentralized manner.
TOKENISATION		Tokenization is the digitalized depiction of an (asset) value, including the rights and obligations contained in this value and its resulting transferability.
TOKENISED COMMERCIAL BANK MONEY	CBMT	See COMMERCIAL BANK MONEY TOKEN
WALLET		A wallet stores public keys and corresponding private keys. Similar to a bank app, a wallet controls access to the account address (the public key). In an amount-based system, wallets do not store tokens because tokens are recorded in addresses on the DLT; a wallet could therefore be seen as a kind of "password manager" because it stores private keys. In a token-based system, wallets may hold tokens. Private keys can be used to sign and correctly execute transactions, and – if valid – to update account balances in the

		DLT. In the case of an offline-capable wallet / prepaid model, the credit balance can also be stored locally. A **hot wallet** is permanently linked to the DLT/blockchain structure (online). The risk of loss is lower than with the cold wallet; in return, the cyber risk is greater. A **cold wallet** is offline, i.e., not connected to the DLT net- work, and the private key for access is on a CD, on paper, or kept on other digital media. A loss of the private key leads to the loss of the assets in the wallet. All the values contained in the wallet would be transferred without being traceable if the wallet is transferred.