Monetary Authority
of Singapore

Purpose Bound Money (PBM) Technical Whitepaper

Contents

Disclaimer

This report and its contents are made available on an "as-is" basis without warranties of any kind. The content in this report does not constitute regulatory, financial, legal or any other professional advice and should not be acted on as such. MAS shall not be liable for any damage or loss of any kind howsoever caused as a result of the use of the information contained or referenced in this report.

Document Version

Version	Date	Author	Rationale
1.0	20 Jun 2023	Monetary Authority of Singapore	First publication

1. Introduction

Digital assets refer to the digital representation of value, such as the ownership of financial assets or real economy assets. The digital asset ecosystem could potentially facilitate more efficient transactions, enhance financial inclusion, and unlock economic value.

Central bank digital currencies (CBDCs), tokenised bank liabilities and potentially well-regulated stablecoins, together with a set of well-designed smart contracts, could serve as the medium of exchange for this new digital asset ecosystem. Although initial trials demonstrate potential, these new forms of digital monies, popularised with the blockchain and peer-to-peer money movement, need to demonstrate their utility above and beyond what is already possible today with e-payment systems such as domestic instant payment systems.

A touted benefit of digital money is its ability to support programmability features. However, this is a subject of ongoing discussion and debate. Operators will need to ensure that programmability does not come at the expense of digital money's ability to serve as a medium of exchange. The singleness of money should be preserved, and programmability should not limit the distribution of money and lead to fragmentation of liquidity in the system.

This paper provides a technical overview to the concept of *Purpose Bound Money (PBM)*, which enables money to be directed towards a specific purpose, without requiring money itself to be programmed. PBM features the use of a common protocol that is designed to work with different ledger technology and forms of money. With a standardised format, users will be able to access digital money using the wallet provider of their choice.

The paper will build upon the concept of PBM, which was first introduced as part of MAS' Project Orchid[1] and describe how it can be extended to a broader set of use cases.

2. Background and Motivation

Digitalisation initiatives aimed at increasing operational efficiency and enhancing user experience have gained significant momentum in recent years. However, digitalisation efforts in the financial sector are not without its challenges.

Proliferation of markets and their fragmentation

The proliferation of payment schemes and platforms increase the complexity and challenge users may face when adopting digital financial services. For example, payment operators often run separate distribution channels with distinct features for different schemes. It is resource intensive for scheme owners to onboard merchants to their proprietary platforms. Meanwhile, integration to additional platforms increases merchants' operation effort and merchants would have to train their retail staff to handle and accept different payment schemes.

Private, independent efforts have sought to consolidate such schemes into a single platform that seeks to streamline the user experience, to realise the potential of digitalisation. However, these efforts

[1] Project Orchid is a collaborative project between MAS and industry partners that aims to build the foundational digital infrastructure and blueprint required for a future digital money ready platform. This paper was adapted from Project Orchid Phase 1 report for a general international audience to facilitate ongoing learning and collaboration.

need to go further to ensure they are open and interoperable across all the schemes. These platforms should not limit access only to consumers and merchants who are subscribed to their ecosystem. Interoperable payments systems will allow greater flexibility and provide a seamless payment experience for businesses and consumers alike.

Programmability and fungibility of money

Unlike traditional account-based ledger systems, digital money offers the possibility of programming unique characteristics into the individual bearer asset and dictate how the digital money is to be used.

However, implementing programming logic directly on a digital money would modify its properties and acceptance as a medium of exchange. While this method expands the capabilities of digital money, it would constrain the use of digital money as a viable medium of exchange if the conditions for its use are varied and dynamic. It would also require re-programming all the digital monies that are in circulation, every time a new condition or use case is required.

An alternative method is for a digital money issuer to provision multiple versions of digital money, each with different logic programmed into it. However, such a method may not be practical as these digital monies would not be fungible with one another and would fragment the liquidity in the market.

To understand how the fungibility of digital money can be retained such that it can be exchanged freely, different programmability models were studied in this paper.

Models of Programmability

Programmable payment[2] refers to the automatic execution of payments once a pre-defined set of conditions are met. For example, daily spending limits or recurring payments could be defined, similar to direct debits and standing orders. Programmable payments are commonly implemented through setting up database triggers or in the form of Application Programming Interface (API) gateways that sit between the accounting ledger and the client application. These programming interfaces interact with traditional ledgers and adjust bank account balances based on programmed logic.

Programmable money[3] refers to the possibility of embedding rules within the store of value itself that defines or constrains its usage. For example, rules could be defined such that the store of value could only be sent to whitelisted wallets or transferred upon completion of transaction level screening. Programmable money implementations include tokenised bank liabilities and CBDCs. Unlike programmable payment, whereby the programming logic and the value itself are decoupled, programmable money is self-contained and contains both programming logic and serves as a store of value. When programmable money has been transferred to another party, the logic and rules are moved as well.

Programmable payment's advantage is its ability to define a set of programming logic or conditions that could be applied across a variety of different forms of money. Meanwhile, programmable money has the advantage of being self-contained and having conditional logic transferrable on a peer-to-peer basis between parties. With central banks, commercial banks and payment service providers globally exploring different CBDCs, tokenised bank liabilities and stablecoin designs, it is envisioned that the future financial landscape will be even more diverse. Consequently, there is a growing need to ensure

[2] In traditional financial technology systems and any "programmability" offered for this money involves another technology system built separately from that database and then connected in some fashion (Lee, 2021).
[3] Programmable money as a unified, coherent product that encapsulates both the storage of digital value and programmability of that value (Lee, 2021).

that there is a common framework for interacting with different forms of digital monies and ensure interoperability with existing financial infrastructure.

A third model – *Purpose Bound Money (PBM)*, which is explored in the initial phase of MAS' Project Orchid, builds upon the concept and capabilities of both programmable payment and programmable money. PBM refers to a protocol that specifies the conditions upon which an underlying digital money can be used. PBMs are bearer instruments, which are transferrable on a peer-to-peer basis without intermediaries. PBMs contain digital money as a store of value and programming logic denoting it's use based on programmed conditions. Once the conditions are met, digital money is released, and it becomes unbounded once again.

This can be illustrated with the example of PBMs being used as a digital voucher. A voucher comes with it a predefined set of conditions for its usage. The holder of the voucher can present it to participating merchants in exchange for goods or services (a programmable payment feature). In some instances, the terms of the voucher scheme allow it to be transferrable between people (a programmable money feature). Hence, a consumer could purchase a PBM based gift voucher and transfer it to another person who may then use it at a participating merchant.

However, unlike a regular voucher, it places constraints on how the payer can use the PBM but there are no constraints on the payee. When a consumer pays for his purchase using PBM, the digital money is released from the PBM and transferred to the merchant if the terms of use are fulfilled. Thereafter, a merchant could use the digital money for other purposes (e.g. to pay a supplier) without any constraints.

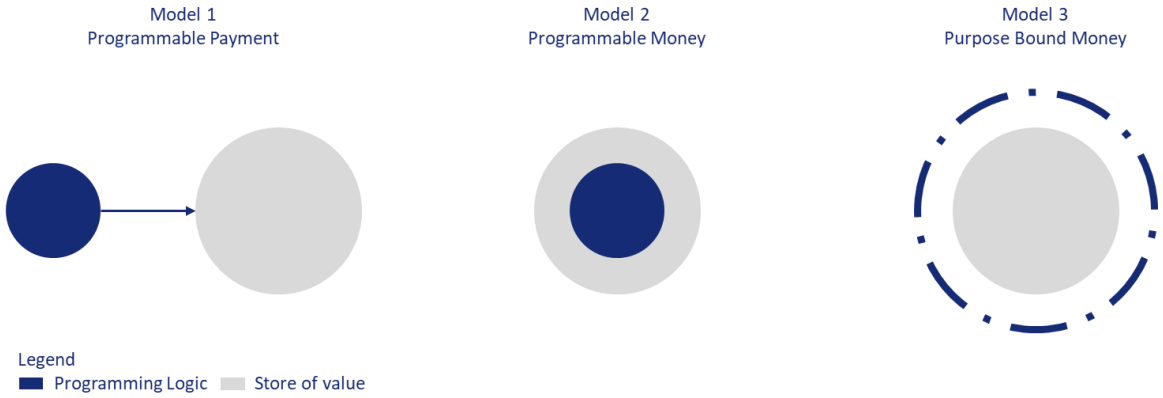

Figure 1: Possible models of programmable digital money

Features	Programmable Payment	Programmable Money	Purpose Bound Money
Programming logic is transferred alongside store of value	No	Yes	Yes
Programming logic may be developed by 3rd party who is not the issuer of the store of value	Yes	No	Yes
Bearer Instrument	No	Yes	Yes

Table 1: Comparison between different models

3. Purpose Bound Money

This section examines the lifecycle of a PBM and the different components that makes up a PBM. In this section, the key entities and their interactions are outlined, emphasising the roles they play within the PBM lifecycle.

3.1. System Architecture Overview

The PBM protocol references a four layered model to describe the technology stack used in a digital asset-based network. The components of the network can be categorised into four distinct layers: access layer, service layer, asset layer, and platform layer, as shown in Figure 2. The programming logic of a PBM may be characterised as a service, while digital money is at the asset layer. When digital money is bound as a PBM, it straddles the service and asset layers.

The PBM design is technology neutral and aims to work across different types of ledgers and assets. It is envisioned that PBM could be implemented on both distributed and non-distributed ledgers.[4]

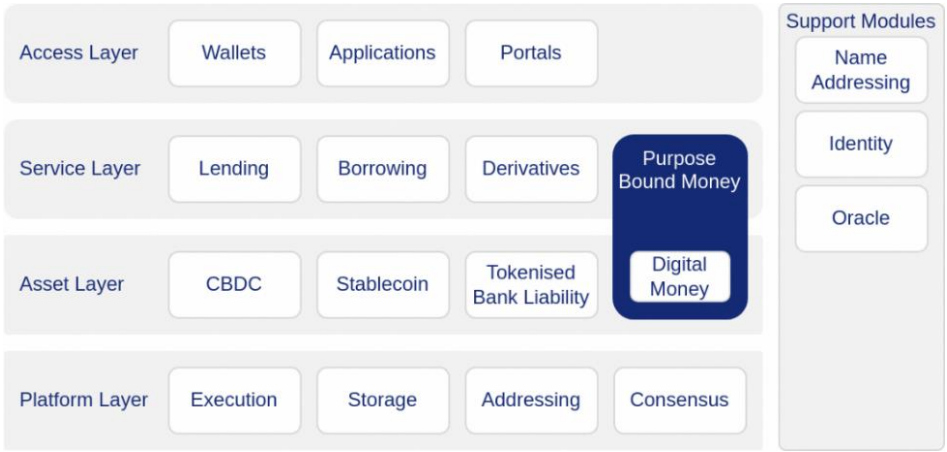

Figure 2: System Architecture Overview[5]

Access Layer

The access layer is a layer through which users interact with various interfaces to access different services.

Service Layer

The service layer provides various services related to digital assets. It typically operates on top of the asset layer and enables users to manage and utilise their digital assets.

Asset Layer

The asset layer enables the creation, management, and exchange of digital assets.

Platform Layer

The platform layer provides the underlying infrastructure for executing, storing, and reaching consensus on transactions.

[4] Programmability and composability do not require decentralised or permissionless platforms (Carstens, 2023).
[5] System architecture jointly developed with International Monetary Fund (IMF).

3.2. Components

A PBM consists of two main components, as shown in Figure 3: a wrapper that defines the intended use; and an underlying store of value that serves as collateral. This design allows for existing digital money to be deployed for different purposes without altering its native property. Once the PBM has been utilised for its intended purposes, the digital money can be used without any conditions or constrains. The digital money issuer retains control over the digital money, preventing fragmentation and ensuring easy maintenance.

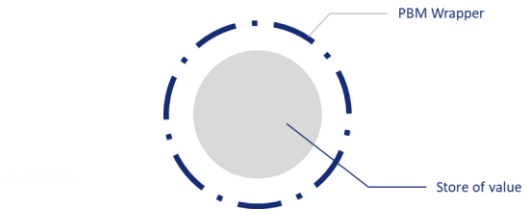

Figure 3: Purpose Bound Money Components

PBM Wrapper

The PBM Wrapper implemented in the form of smart contract code, specifies the conditions upon which the underlying digital money can be used. The PBM Wrapper could be programmed whereby the PBM can only be utilised for its intended purposes, such as validity within a certain period, at specific retailers, and in predetermined denominations. Once the conditions specified in the PBM Wrapper are met, the underlying digital money will be released and transferred to the recipient. For example, the PBM wrapper could be implemented as an ERC-1155[6] multi token smart contract. Section 3.5 shows the sequence flow of one possible design of PBM.

Digital Money

The underlying digital money bound by a PBM serves as a collateral for the PBM. When the conditions of a PBM are fulfilled, the underlying digital money is released, and ownership is transferred to the target recipient. The digital money must meet the functions of money, namely as a good store of value, a unit of account, and a medium of exchange. Digital monies could come in the form of CBDCs, tokenised bank liabilities or well-regulated stablecoins. As an example, digital money could be implemented in the form of an ERC-20[7] compatible fungible token smart contract.

3.3. Roles and Interactions

A role, being a flexible abstraction, can be realised in various ways. It is possible for an entity to hold multiple roles or for a role to be performed by different entities.

PBM Creator

This entity is responsible for defining the logic within the PBM, minting, and distribution of the PBM tokens.

[6] ERC-1155 is an interface to manage multiple token types (e.g., fungible, non-fungible, semi-fungible).
[7] ERC-20 is commonly used to implement fungible tokens.

PBM Holder

This entity holds one or more PBM tokens. This entity can redeem non-expired PBM tokens.

PBM Redeemer

This entity receives the underlying digital money when PBM tokens are transferred.

3.4. Lifecycle

The PBM is designed to have consistent lifecycle stages, irrespective of the programming language or network protocol used, ensuring compatibility across different technical implementations. This section provides an overview of the expected functionalities and associated lifecycle stages of the PBM. Figure 4 shows the different stages in a PBM lifecycle.

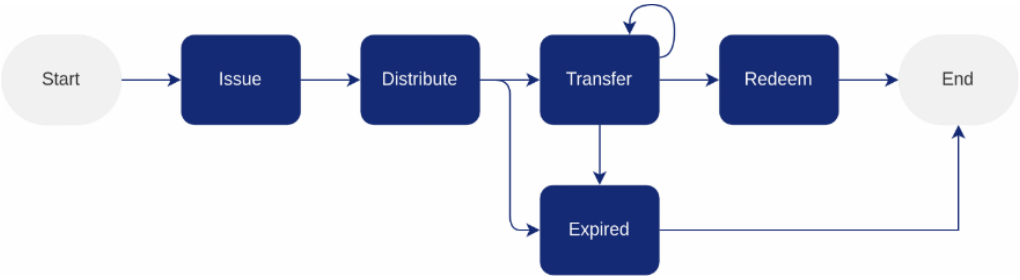

Figure 4: PBM Lifecycle

Issue

The PBM lifecycle starts with the issue stage. Here, a PBM smart contract is created, and PBM tokens are minted. The ownership of a digital money is transferred to the PBM smart contract. The digital money is now bound by the PBM smart contract, which may be implemented using ERC-1155 or equivalent. The usage of the digital money is governed by the conditions specified in the PBM smart contract and will only be released upon fulfilling all the conditions.

Distribute

After the PBM tokens are minted, they are distributed by the PBM Creator to the intended entities (i.e., PBM Holders) for usage. The PBM Holder receives the PBM tokens in its wrapped form and can only redeem the tokens according to the original conditions set by the PBM Creator.

Transfer

In this stage, PBM tokens may be transferred from one entity to another in their wrapped form and according to its programmed rules. The transfer stage is optional, depending on the use case. In a government disbursement (e.g., study grant), PBM tokens may not be transferrable to other citizens. Whereas in a commercial voucher (e.g., retail mall vouchers), PBM tokens can be transferred to other consumers.

Redeem

The redeem stage occurs after all the conditions specified in a PBM have been fulfilled. At this point, the PBM token is unwrapped, and ownership of the underlying digital money token is transferred to the receiving entity. The entity can freely utilise the digital money token, with its usage constrained only by the conditions specified by the digital money issuer.

Expired

The expired stage refers to situations where one of the conditions specified in the PBM have unmistakably been violated or expired (e.g., expiry date), rendering the PBM token to be permanently unusable for the PBM Holder. Expired PBM tokens can be aggregated and destroyed or "burnt" to return the underlying digital money to the PBM Creator. Alternatively, the PBM can be paused indefinitely to prevent further interaction with the expired PBM by the PBM Holder.

3.5. Sequence Flow

PBM implementation can vary in terms of design, approaches, and technology. In this section, we explore one design where the PBM is divided into three components, as shown in Figure 5. In this implementation, the following conditions have been defined for the release of the digital money: (1) access control via whitelisting and blacklisting; (2) PBM Wrapper expiry date; and (3) PBM token type expiry date.

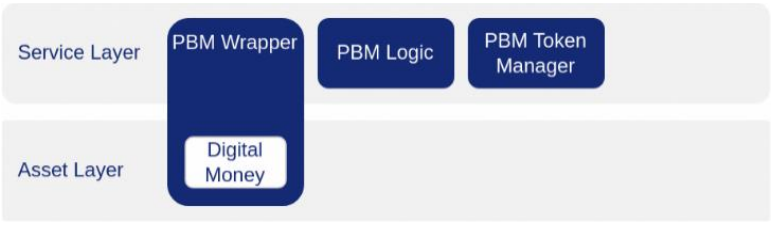

Figure 5: PBM Smart Contracts

PBM Token Manager

For example, if the ERC-1155 multi token standard was adopted, the PBM Creator can create different PBM token types representing different values within the same PBM Wrapper (e.g., $1, $2, $5, etc). The PBM token manager provides an interface to easily manage the different token types and maintain the balance of each token type. The following are some of the key functions of this component:

1. Create PBM token types.
2. Get the details of each PBM token type.
3. Increase/decrease supply balance of each PBM token type.
4. Validate PBM token expiry.

PBM Logic

This component allows users to create complex business conditions while keeping the PBM Wrapper lean. In our example, this component stores and manages a list of whitelisted and blacklisted addresses. The following are some of the key functions of this component:

1. Add or remove address from whitelist.
2. Add or remove address from blacklist.
3. Check if PBM token can be transferred.
4. Check if PBM token can be unwrapped.

PBM Wrapper

This component contains the conditions governing the usage of the underlying digital money. The digital money can be ERC-20 compatible and may take the form of a CBDC, tokenised bank liabilities or stablecoin. For illustration purposes, the PBM Wrapper was assumed to be implemented using the ERC-1155 multi token standard. Other standards like ERC-20, ERC-721 or their equivalents can also be used for implementation. The following are some of the key functions of this component:

1. Minting of PBM tokens.
2. Burning of PBM tokens.
3. Transfer PBM tokens.
4. Interacting with PBM Logic component for additional validations.
5. Interacting with PBM Token Manager for PBM token type management.

Figure 6 shows the interaction between the different PBM smart contracts. In the subsequent sections, we present a detailed sequence flow for each stage of the PBM lifecycle.

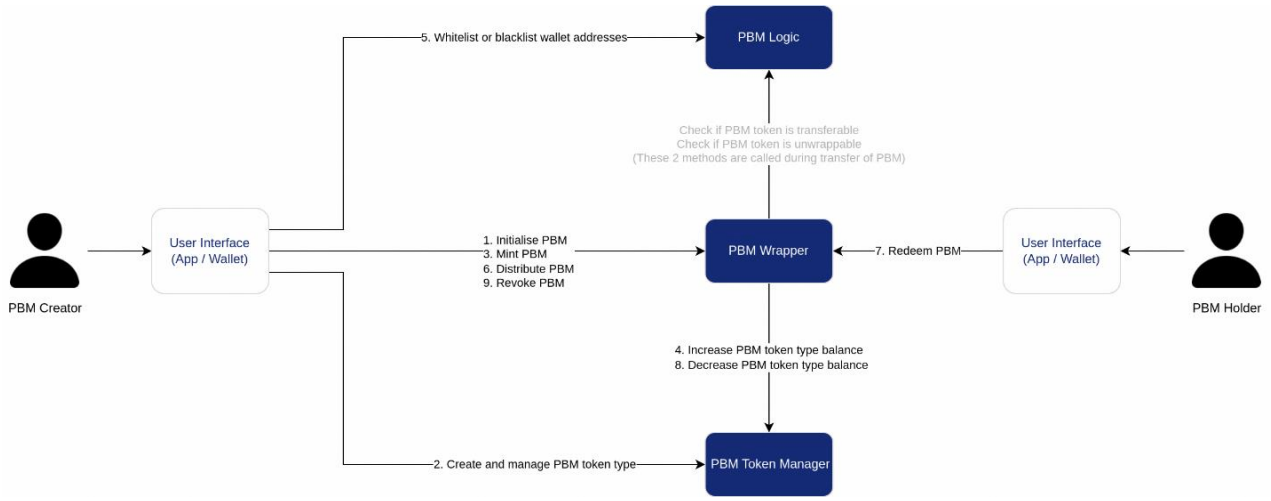

Figure 6: PBM Smart Contracts Relationship

PBM Lifecycle: Issue Stage > Initialise PBM

Figure 7 illustrates the steps to initialise the PBM smart contract. In this stage, the PBM Creator provides different parameters to initialise the PBM and setup the connection between the different PBM components.

Figure 7: Initialise PBM Smart Contract

PBM Lifecycle: Issue Stage > Create PBM Token Type

Figure 8 illustrates the steps to create new PBM token type. In this stage, the PBM Creator can create different token types representing different values.

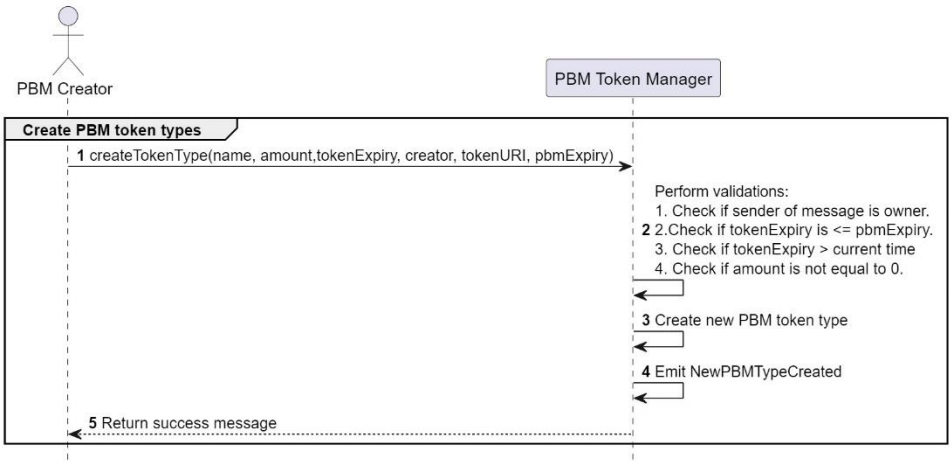

Figure 8: Create PBM Token Types

PBM Lifecycle: Issue Stage > Minting of PBM Tokens

After the above steps, the PBM Creator can start to mint the PBM tokens for distribution. Figure 9 shows the steps in the minting of PBM tokens.

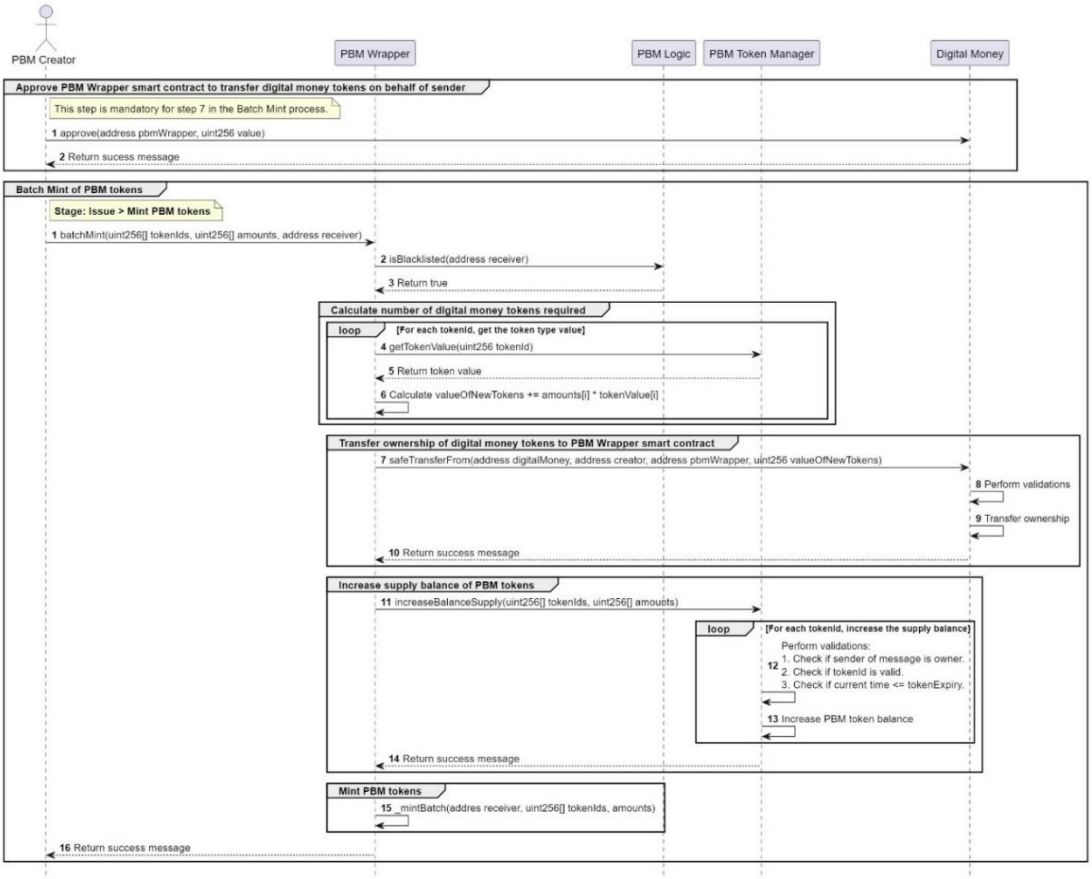

Figure 9: Mint PBM Tokens

- Prior to the minting process, the PBM Creator must approve the PBM Wrapper smart contract the rights to transfer the digital money on behalf of the PBM Creator. This is a mandatory step for Step 7 of the minting process to run.
- Step 1: PBM Creator initiates the batch minting process.
- Step 2: As it is possible to mint and distribute in one single transaction, the PBM Wrapper must call PBM Logic to check if the receiver is blacklisted.
- Steps 4 to 6: Calculate the total number of digital money tokens required for minting the PBM tokens.
- Steps 7 to 10: Transfer ownership of digital money tokens to the PBM Wrapper as collateral.
- Steps 11 to 14: Increase the supply balance of the PBM token types.
- Step 15: Mint PBM tokens.

Whitelist/Blacklist Address

The PBM could be programmed with conditional logic to check the set of addresses that are allowed to receive the tokens and which are the ones that are not. In our example, a PBM token cannot be transferred if the receiver is blacklisted. A PBM token cannot be unwrapped if the receiver is not whitelisted. The PBM Creator can access the below functions throughout the lifecycle of the PBM. It is important to note that distribute and transfer stage is the same flow technically and only differs by the roles involved. If a PBM is distributed to a whitelisted address, the PBM will unwrap and release the digital money.

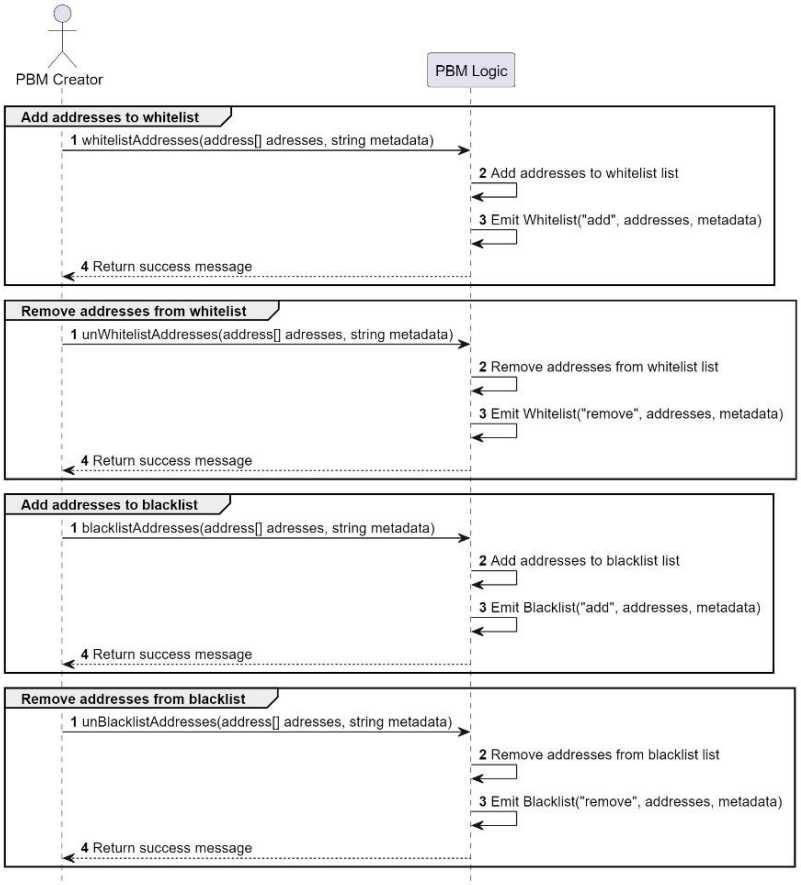

Figure 10: Add or remove address from whitelist or blacklist

PBM Lifecycle: Distribute / Transfer

In either the Distribute or the Transfer stage, the PBM tokens are transferred in its wrapped form. The only difference between the two stages are the roles involved. Figure 11 illustrates the steps involved.

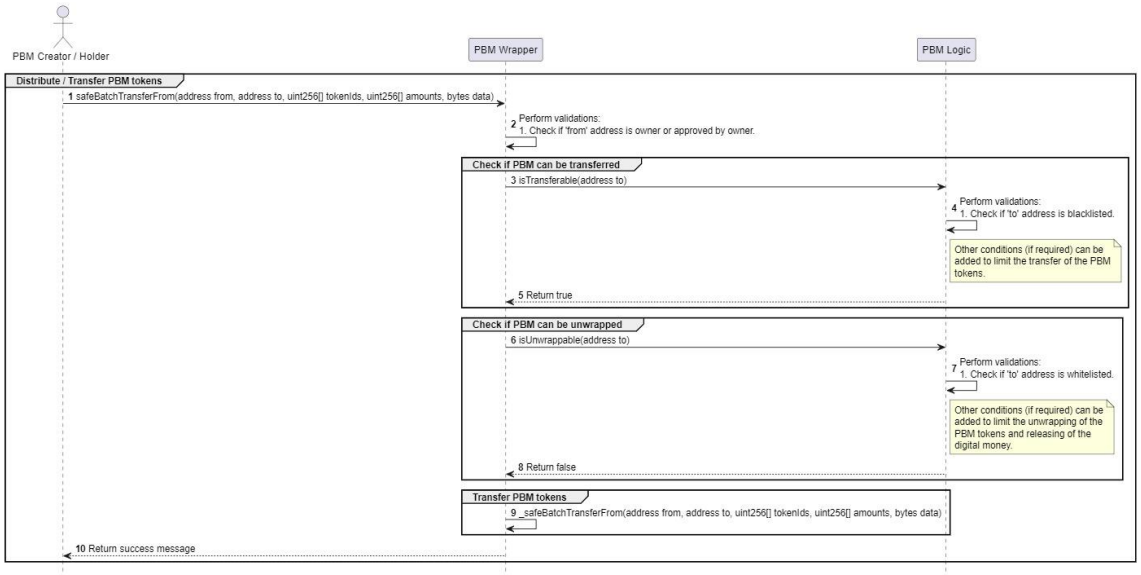

Figure 11: Distribute or transfer PBM tokens

The following outlines some of the key steps and its considerations during the transfer of the PBM tokens.

- Steps 3 to 5: Check if PBM tokens can be transferred. Additional conditions can be added here. In our example, check if the receiver has been blacklisted.
- Steps 6 to 8: Check if PBM can be unwrapped to release the digital token. Additional conditions can be added here. In our example, the receiver needs to be whitelisted.
- Step 9: Transfer PMB tokens in wrapped form.

PBM Lifecycle: Distribute / Transfer – Unsuccessful Transfer

Figure 12 illustrates the steps for an unsuccessful transfer of PBM tokens. The PBM tokens are not transferred and stays in its wrapped form.

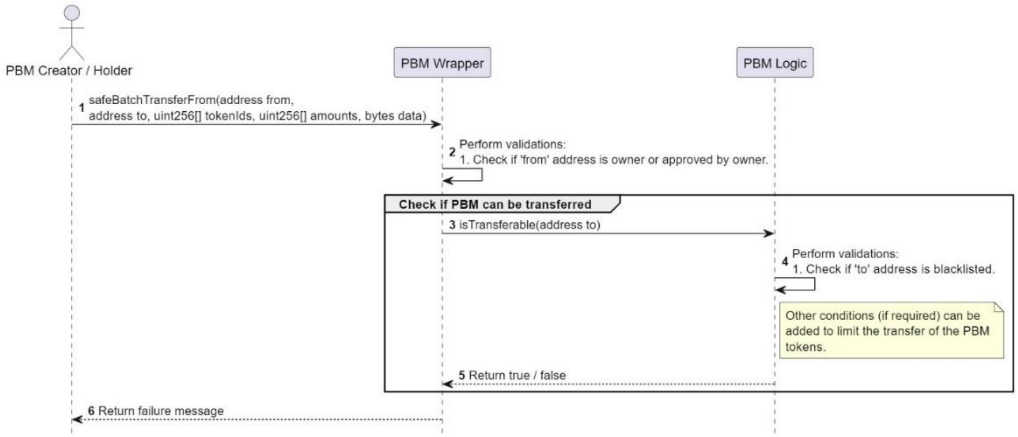

Figure 12: Failed to distribute or transfer PBM tokens

PBM Lifecycle: Redemption Stage

During the transfer of the PBM token, if all the conditions are fulfilled, the PBM token unwraps and release the underlying digital money token to the receiver.

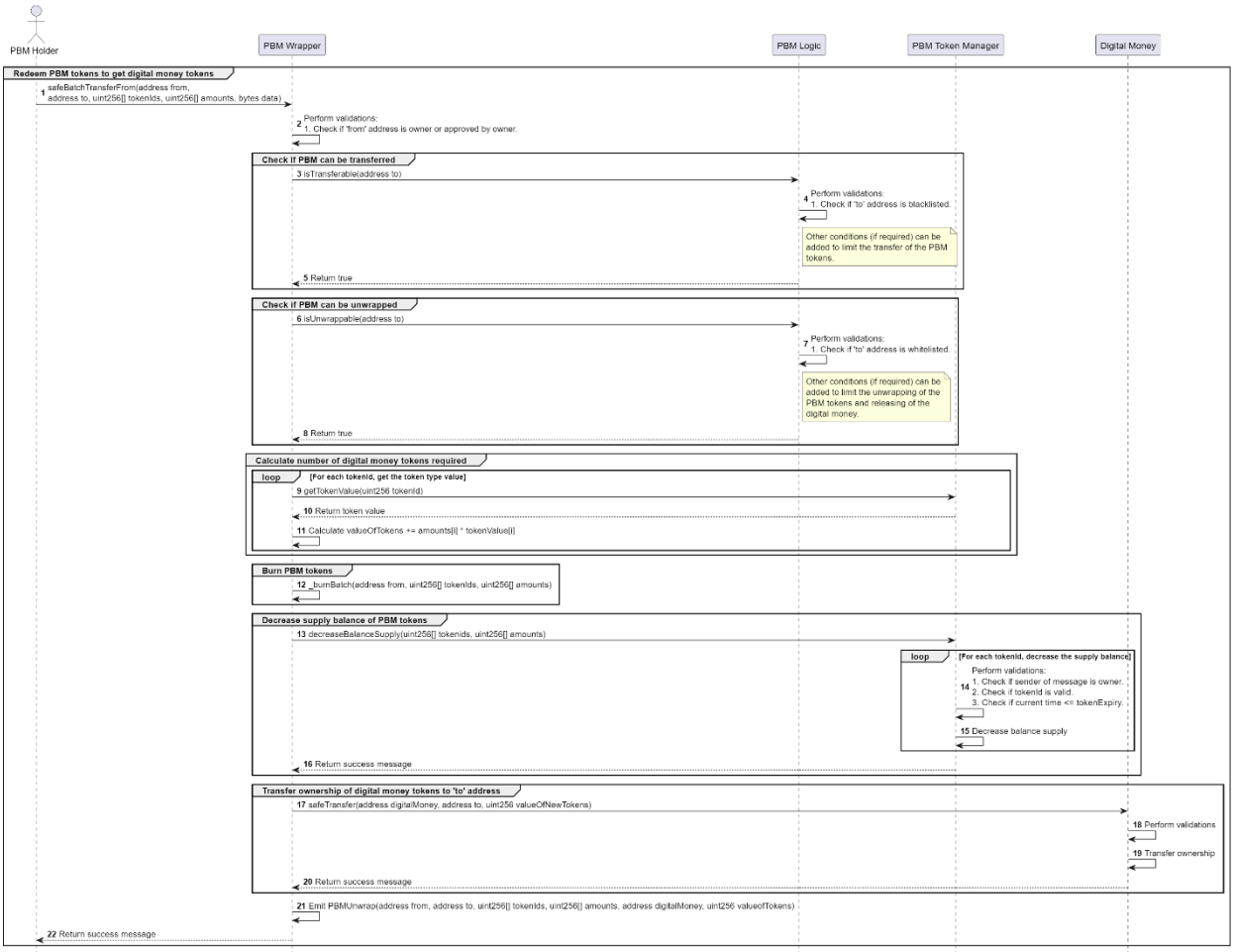

Figure 13: Redeem PBM tokens

The following outlines some of the key steps and its considerations.

- Steps 6 to 8: Check if PBM token can be unwrapped to release the underlying digital token. If all the conditions are fulfilled, the PBM token can be unwrapped. In our example, check if receiver has been whitelisted.
- Steps 9 to 11: Calculate the amount of digital money tokens to transfer to the receiver.
- Step 12: The PBM token is burnt. This step is optional and depends on the requirements of the PBM Creator. In some scenarios, the PBM token might be kept for commemorative purposes.
- Steps 13 to 16: The number of PBM tokens are decreased. In our design, the validation of the expiry date of the token is performed in step 14 instead of step 7. This is because the token manager is designed to manage all aspects of the PBM tokens as per our design. Others may implement the validation in step 7 instead.
- Steps 17 to 20: The PBM Wrapper transfers its ownership of the digital money tokens to the receiver.
- Step 21: Emits the PBMUnwrap event.

PBM Lifecycle: Expired Stage > Redeem expired PBM token

At this stage, the PBM Holder tries to redeem a PBM token where at least one of the conditions has been unmistakeably violated or expired, and the transfer fails. In our example, the token has expired. The following outlines some of the key steps and their considerations.

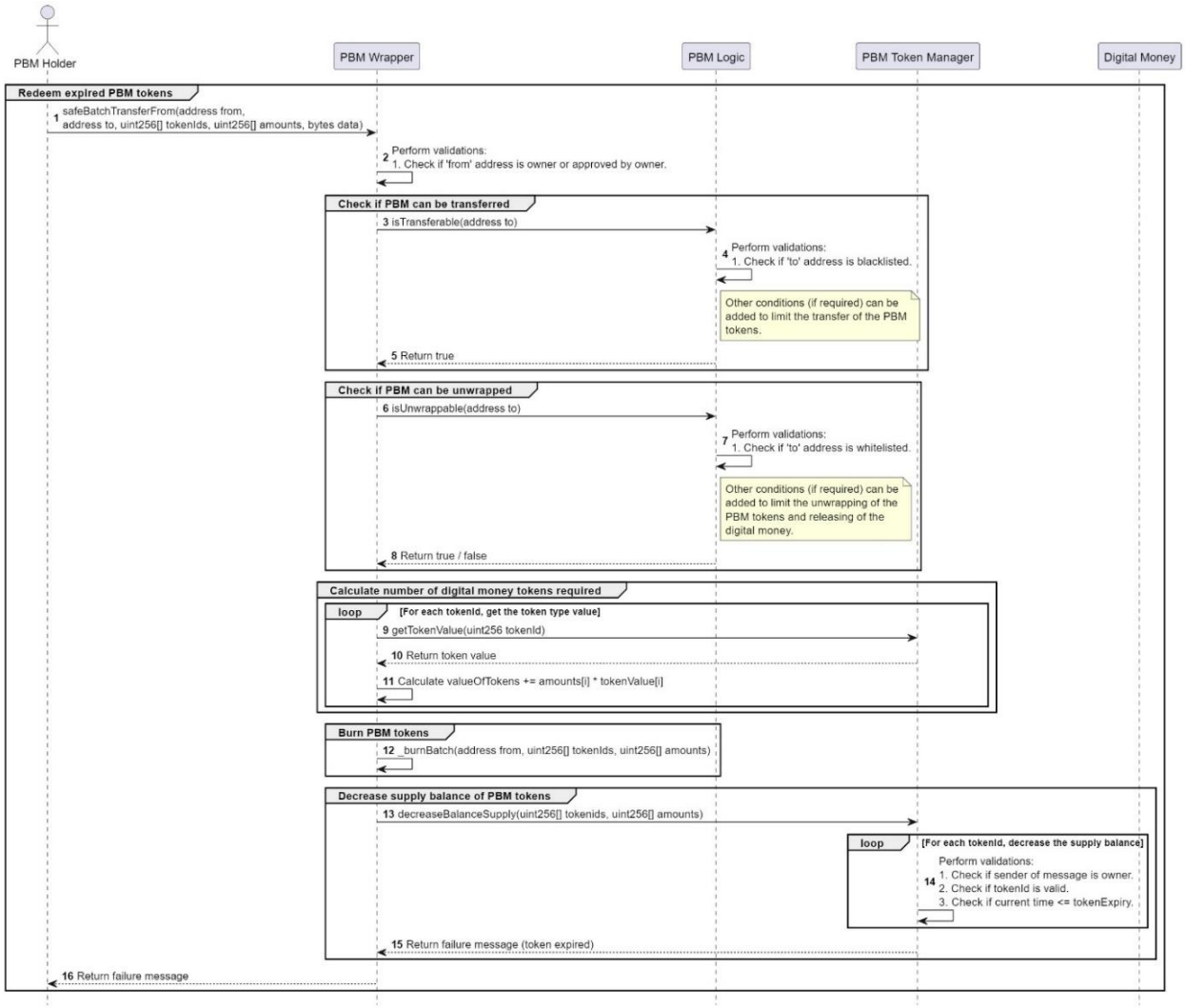

Figure 14: Redeem expired PBM token

- Steps 6 to 8: The PBM token is treated as unwrappable as we have implemented the validation of the token expiry in step 14 as explained in the redemption stage.
- Step 14: The validation failed as the token has expired.

PBM Lifecycle: Expired Stage > Revoke PBM

The PBM Holder cannot utilise the PBM tokens if at least one of the conditions has been unmistakeably violated or expired, and the digital money remains locked. In our example, the token has expired. The PBM Creator has the option to revoke expired PBM tokens to recover the underlying digital money tokens.

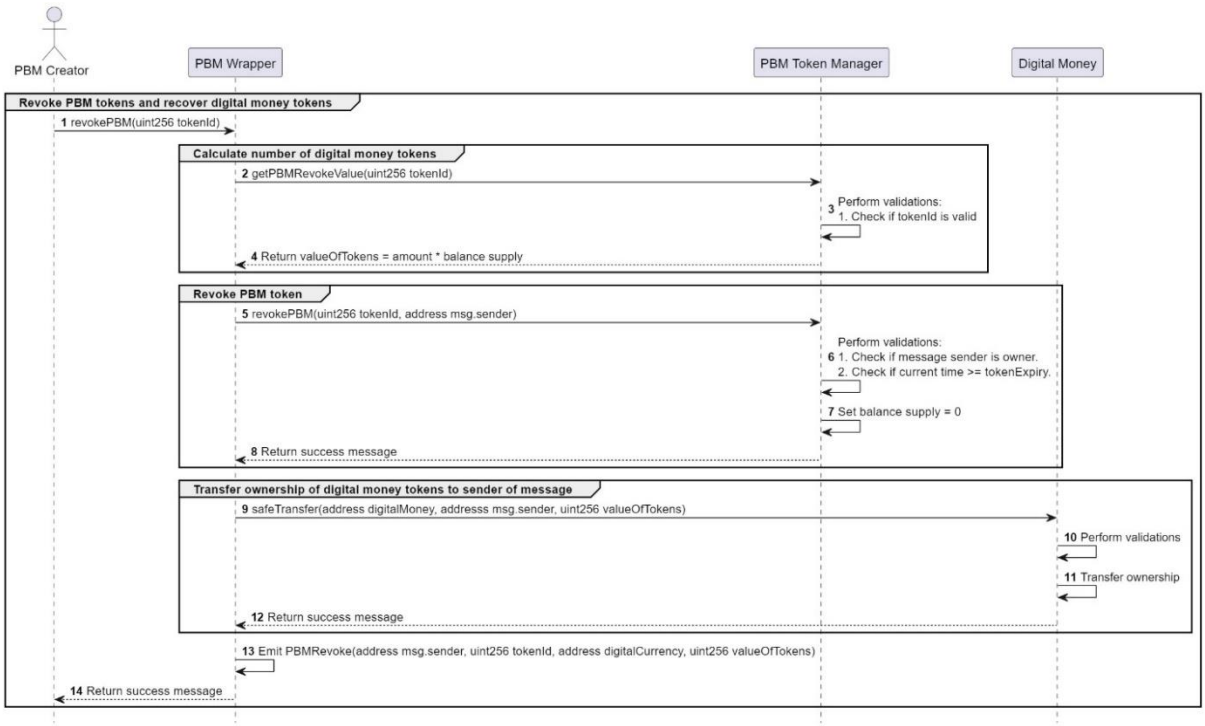

Figure 15: Revoke expired PBM tokens

- Step 1: The PBM Creator initiate the revocation.
- Steps 2 to 4: Calculate the amount of digital money tokens to retrieve.
- Steps 5 to 8: Revoke and set token balance to 0.
- Steps 9 to 12: Transfer the digital money token to the PBM creator.
- Step 13: Emit PBM revocation event.

4. Design Considerations

This section discusses some of the design choices and factors that might weigh into how a PBM might be implemented.

Interoperability

It is critical that the implementation of PBMs by different service providers does not lead to fragmentation in the payment ecosystem. PBM providers running their own proprietary networks could lead to the creation of “walled gardens” within their own closed ecosystem of partners. This could lead to monopolistic, rent-seeking behaviour amongst PBM providers. If left unchecked, this could be to the detriment of consumers, who will either need to onboard to a myriad of different systems or pay exorbitant fees to intermediaries to complete a transaction.

Hence, it is prudent for PBM technology to be designed at the onset to be interoperable across different platforms, wallets, payment systems and rails. This will enable PBM recipients to access and use their PBM tokens from a government provided or commercial wallet provider of their choice. The adoption of a common standard ensures that PBM tokens are compatible with different wallet service providers. This will enable digital assets to be transferred across different platforms and stakeholders. Furthermore, the effort and cost of implementation is reduced as the same infrastructure can be reused across multiple uses cases.

The PBM design in this paper is designed to work across a variety of different ledger types, including blockchain and non-blockchain based ledger systems. To illustrate the concepts in this paper, specific technical implementations were provided as examples. It is envisioned that future implementations of PBM could be based on a different ledger system from the ones referenced in this paper. Service providers will need to choose the supporting ledger type that best suits their business model and intended use cases.

Digital Money

Conceptually, PBM provides a common framework regardless of the type of underlying digital money. Since PBMs derive their value from the underlying digital money, the acceptance, perceived value, and usability of PBMs is strongly correlated with the associated digital money.

Hence, it is crucial to consider the reserve assets backing the digital money, as well as their associated regulatory implications and compliance requirements. CBDCs, tokenised bank liabilities and stablecoins offer different levels of guarantees and are subject to different regulatory oversight.

A variation of PBM may be in the form of a purpose bound token, where the underlying digital money is replaced by a token representing an obligation to pay, rather than a store of value. Although this may serve a similar function in terms of representing a contingent liability, settlement is performed on a deferred basis instead of an atomic and real-time basis and is thus subject to risk of settlement failures.

As the global regulatory landscape for digital monies is still evolving, the regulatory treatment of PBMs may vary across jurisdictions.

Privacy

The composable nature of the PBM design means that it is possible for the PBM Wrapper smart contract to be developed by a private sector entity, while using a CBDC that is issued by a central bank as the underlying digital money. Conversely, a government agency may develop the PBM Wrapper smart contract and issue a PBM to support government disbursements using private money in the form of tokenised bank liability as collateral for the PBM.

By separating the role of the PBM Creator and that of the digital money issuer, it is possible to establish an arrangement whereby no single entity has oversight over both the issuance of money as well as how and where money is used. Consequently, the amount of data that is held by individual institutions is limited only to information that is required to perform its authorised function.

As an additional safeguard, it may be possible to setup arrangements where fund transfers can be conducted anonymously but only by authorised entities. For example, before a transfer is made, a PBM condition could be setup where a check is made against a separate registry to ensure the individual initiating the transfer is authorised to make the transfers. However, the registry system in this example has neither oversight over the nature of the transfers nor who is the intended beneficiary. The registry only informs if a party is authorised or not.

Policy Considerations

PBMs could be utilised by the official sector[8] as well as the private sector. While the technical implementation of PBMs may be similar across use cases, there may be additional policy considerations when it is developed, managed, and used by the official sector.

There are differing views internationally on the extent to which constrains should be placed on how individuals spend money. For example, during the disbursement of monies during pandemic, some jurisdictions allow disbursement to be used to purchase financial products and services while other jurisdictions restrict its usage[9]. Meanwhile, some central banks have indicated they would not set any limitations on how digital money can be used.[10].

Consequently, when designing PBM based solutions, policymakers need to consider who should issue and distribute digital monies, as well as specify the conditions for its use.

Digital Readiness

The introduction of new forms of payment instrument would likely change users' experiences and require some adjustment and getting used to. This might be viewed positively by some users and disruptive by others. For example, some merchants and citizens might be more accustomed to using paper vouchers and may not be familiar with mobile apps. This could discourage merchants and citizens from adopting PBM.

Hence, the digital savviness of the stakeholders should be factored into the design of the PBM scheme. It is important that special care be made to keep the user experience intuitive and accessible especially to more vulnerable segments of the population.

An approach is to provide a simplified user experience at the onset, while abstracting away the complexity of requiring a user to manage their own keys to access the digital money or PBMs. Additionally, the PBM could be designed to be interoperable with existing payment rails, thereby reducing frictions in the last mile fiat settlement and merchant acceptance.

Secure Programming

Given the heavy reliance on smart contract code, it is crucial to establish a governance framework that ensures the safety of the code as part of the software deployment process. This can be achieved by engaging trusted entities charged with the task of verifying the correctness of logic, assessing, and preventing potential vulnerabilities, and providing standardised oracle data.

This framework should be applied across the digital money layer as well as the PBM Wrapper smart contract. This becomes particularly important when a PBM Creator aspires to integrate complex logic into components, such as delayed transfers or supply chain payment management. To proactively mitigate potential system security risks, such as the introduction of malicious code, it is highly recommended to conduct an independent audit. Furthermore, for distributed ledger-based networks, a trusted third-party organisation could be engaged to function as an 'oracle', offering dependable external data inputs into the network.

[8] Official sector refers collectively to general government, central banks, and international organisations (BIS, 2019).

[9] Disbursement can be used for primary needs like food, energy bills or gas supplies but forbidden for use in activities (Republic of Italy, 2019).

[10] The digital euro: our money wherever, whenever we need it (Panetta, 2023).

5. Potential Uses of PBM

This section provides examples of how PBM could be used.

Pre-paid Packages

Consumers stand to lose the deposits they have made upfront, as payment for goods and services awaiting future delivery, if the merchants they were dealing with went out of business. PBM could be used in scenarios when corporations require fees to be collected upfront as assurance before manufacturing a good or providing a service. PBM may solve the risk of non-delivery by including conditions for payment, ensuring corporations fulfil their obligations before they "drawdown" on the amount pre-committed by the consumer. The funds drawdown could be automatically triggered (direct debit from consumers PBM e-wallet) after fulfilment of service. While corporations do not get the fees upfront, they have assurance that they would be paid once the service has been rendered.

Online Commerce

When shopping online, consumers are typically required to pay in advance for the product they wish to purchase. Once the payment has been made, the product is shipped to the consumer. To mitigate the risks of non-delivery or payment, consumers and merchants may use a variety of arrangements. Credit cards and forms of pre-payment protect the merchants but not the consumers. Meanwhile, cash on delivery arrangements may be favourable to consumers but offers no assurance to merchants, especially for perishables like food items that cannot be repurposed. PBM offers an alternative solution and provide assurance to both merchants and consumers that funds will be transferred when service obligations are met.

Contractual Agreements

When a homebuyer initiates an application to buy a property, there are different milestone events upon which payments need to be made. A PBM could be created based on terms stipulated with the sale of the property. The terms could be defined such that funds are released at different stages of the property development or stages of the sales process when milestones have been attained. In practice, the PBM could be based off a standard template common across homebuyers.

Commercial Lease

When leasing a property, landlords may require tenants to provide a security deposit as a form of protection against any damages or unpaid rent. This deposit is held by the landlord for the duration of the lease and is returned to the tenant at the end of the lease term, provided that the tenant has fulfilled all their obligations under the lease agreement. If the tenant has caused damage to the property beyond normal wear and tear, or if they have failed to pay fees owed under the lease agreement, the landlord may deduct the cost of repairs or unpaid rent from the security deposit before returning any remaining funds to the tenant. PBM could fulfil the role of security deposits where parties to the lease agreements are guaranteed the possibility of recovering security deposits in full. In cases of disputes, the PBM could be paused till the dispute is resolved.

Trade Finance

Trade finance products help businesses manage the risks and complexities of international trade transactions. To facilitate trade involving multiple parties across different borders and currencies, trade finance providers offer a range of services, such as letters of credit, bank guarantees, and documentary collections. These services help to ensure that payments are made securely and efficiently, while also providing protection against the risks of non-payment or fraud. Trade finance

instruments could be modelled as PBMs whereby payment is automatically made upon fulfilment of service obligations. They could potentially serve as a negotiable instrument that is transferable across parties.

Donations

Potential donors may be hesitant to contribute to social causes because they are not certain if their donations reach the intended beneficiaries and are used for their intended purposes. Furthermore, donations made to overseas beneficiaries in remote areas are likely to involve multiple intermediaries as there are limited economically viable options to remit funds. Consequently, beneficiaries might ultimately receive a donation that is a small fraction of the original value donated. PBMs may be used to facilitate greater transparency and accountability. For example, PBMs could be used to ensure that only the intendent beneficiary can spend the money and only when certain conditions are met.

Cross-border Payments

Cross-border payments are subject to policy and regulatory requirements such as capital flow management and macro-prudential policy measures, as well as anti-money laundering (AML) and combating the financing of terrorism (CFT) standards. Compliance with these measures and standards incurs high costs and processing delays. By embedding existing policy requirements as conditions into PBMs, compliance checks can be automated, thus greatly reducing the costs and increasing efficiency in cross-border payments. This compliance-by-design approach could contribute to regulatory and policy interoperability in the context of the G20 roadmap to enhance cross-border payments.

6. Future Work

Developments in digital money space are rapidly evolving. In this section, potential future research areas are discussed.

Account Abstraction

Currently, most retail users are not familiar with the use of digital asset wallets and this unfamiliarity could increase the risk of exploits by malicious actors. To mitigate this, account abstraction, also known as smart contract wallets, can be used to improve the user experience and security of digital asset transactions. This technology allows for features such as account recovery, transaction limits, and freezing of lost accounts, without requiring users to understand the underlying technology.

Offline Payment

Future research may include studying the use of PBM for non-smartphone-based form factors (e.g., cards), as well as offline payment to reduce reliance on network connectivity. This is aimed at improving financial inclusion and enabling people to participate without requiring access to smartphones or digital payment services.

Name Addressing

At present, fund transfers can be performed using mobile numbers as a proxy for bank account numbers. In the absence of bank accounts numbers, a name addressing service provides a proxy to a wallet address by mapping it to a meaningful identifier. This could give a better user experience and ensure that the transfer is made to the intended recipient.

7. Conclusion

This paper proposed the concept of PBM as a common protocol for interacting with different forms of medium of exchanges, and highlights how digital money can be used to support commercial and policy objectives without modifying its native properties. While PBM was first introduced through MAS' Project Orchid, it is envisioned that the technical design concepts may be applicable for a broader audience internationally.

To realise wider adoption, the PBM technical framework is designed and developed in an open-sourced manner with participation across different organisations. The paper builds upon the foundational work started with Project Orchid and is the result of the collective contribution from central banks, financial institutions and FinTech around the world.

It is important to note that this paper does not seek to advance any specific policy objectives or endorse any technical solution. The authors of this paper make no representation or guarantees on the performance or adequacy of the proposed solution. Examples provided in the paper are purely for illustration purposes. As the policy consideration and landscape in each jurisdiction is unique, decision makers will need to assess the combination of financial infrastructure and technology that best aligns to their objectives.

It is foreseeable that future developments in digital money and digital assets ecosystem may introduce additional opportunities and surface risks that will need to be addressed in future work. Members of the global FinTech community are encouraged to build upon the concepts introduced in this paper and contribute the learning points back to the global FinTech community.

References

1. Monetary Authority of Singapore (MAS). (2022, October 31). Project Orchid: Programmable Digital SGD [PDF]. Retrieved from https://www.mas.gov.sg/-/media/mas-media-library/development/fintech/project-orchid/mas-project-orchid-report.pdf
2. Lee, A. (2021, June 23). What is Programmable Money. Retrieved from https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.html
3. Repubblica Italiana [Republic of Italy]. (2019, April 19). Decree 19 aprile 2019: Utilizzo della Carta Reddito di Cittadinanza [Decree 19 April 2019: Use of Citizenship Income Card]. Gazzetta Ufficiale. Retrieved from https://www.gazzettaufficiale.it/eli/id/2019/06/26/19A04119/sg
4. Reserve Bank of India. (2022, October 7). Concept Note on Central Bank Digital Currency, Item 5.7: Programmability. Retrieved from https://rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1218#CP57
5. Panetta, F. (2023, January 23). The digital euro: our money whenever, wherever we need it [Speech]. Presented at the Committee on Economic and Monetary Affairs of the European Parliament. Retrieved from https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230123~2f8271ed76.en.html
6. Bank for International Settlements. (2019, April 1). “Official sector” in “Glossary”. Retrieved from https://www.bis.org/statistics/glossary.htm?&selection=272&scope=Statistics&c=a&base=term
7. Carstens, A. (2023, February 22). Innovation and the future of the monetary system [Speech]. Presented at the Monetary Authority of Singapore. Retrieved from https://www.bis.org/speeches/sp230222.htm
8. Adrian, T., & Mancini Griffoli, T. (2023, June 19). The Rise of Payment and Contracting Platforms [PDF]. Retrieved from https://www.imf.org/-/media/Files/Publications/FTN063/2023/English/FTNEA2023005.pdf
9. Bank for International Settlements. (2023, June 20). III. Blueprint for the future monetary system: improving the old, enabling the new [PDF]. Retrieved from https://www.bis.org/publ/arpdf/ar2023e3.pdf

Appendix

Contributors

International Bodies and Central banks	
1	Banca d'Italia
2	Bank of Korea
3	International Monetary Fund
4	Monetary Authority of Singapore
Industry Partners	
1	Amazon
2	DBS Bank Ltd
3	Fazz Financial Group Pte. Ltd.
4	Grab Holdings Ltd.
5	Onyx by J.P. Morgan
6	Network for Electronic Transfers (NETS)
7	OCBC Bank
8	Open Government Products, Government Technology Singapore
9	United Overseas Bank Limited