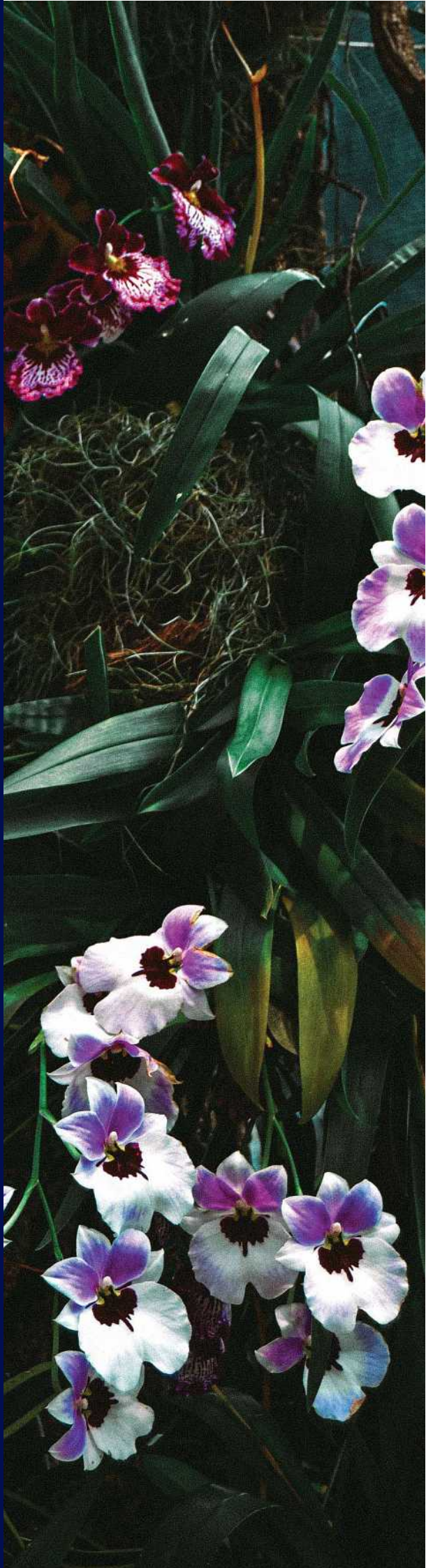
Monetary Authority of Singapore

Project Orchid

Programmable Digital SGD



Contents

Foreword

Digital assets enabled through the innovative combination of tokenisation and distributed ledgers offer transformative economic potential. Tokenisation enables anything of value to be represented in digital form, stored and exchanged on a ledger that keeps an immutable record of all transactions. If done right, the digital asset ecosystem could potentially facilitate more efficient transactions, enhance financial inclusion, and unlock economic value. It could improve financial services – a common goal shared by MAS, the financial industry and the FinTech community. However, like all innovations, digital asset activities pose risks as well as benefits.

MAS' vision is to build an innovative and responsible digital asset ecosystem in Singapore. The development strategy and regulatory approach for digital assets go hand-in-hand towards achieving this. MAS' development strategy makes Singapore one of the most conducive and facilitative jurisdictions for digital assets. At the same time, MAS' evolving regulatory approach makes Singapore one of the most comprehensive in managing the risks of digital assets, and among the strictest in areas like discouraging retail investments in cryptocurrencies.

Innovation through industry collaboration is key to growing the digital asset ecosystem. To support the development of a digital asset ecosystem, we need the supporting infrastructure for mediums of exchange to facilitate transactions. An ongoing focus for MAS is to strengthen our digital currency connectivity by developing the infrastructure and technical competencies necessary to issue a digital Singapore dollar (SGD).

However, the only way to find out what works is through experimentation and exploration – "learning by doing". Policy makers and institutions could benefit from building their own archetypes of possible design choices for a digital currency-based infrastructure to promote debate and innovation moving forward.

Project Orchid and its experiments are a step forward in advancing the global learning on the possibility of programmable money and payments. Rather than building a Central Bank Digital Currency (CBDC) ledger first, the project has taken a user driven approach instead. The first phase of the project aims to uncover a potential use cases for a programmable digital SGD and the infrastructure required. The subsequent phase of Project Orchid will investigate the optimal ledger technology to issue a CBDC as well as its integration to existing financial market infrastructure.

The project seeks to approach the subject of enabling an innovative, interoperable, and inclusive digital currency infrastructure in an open-sourced manner, with a view of harnessing collective contributions of the community and contributing the learning points to the global FinTech community.

SOPNENDU MOHANTY

CHIEF FINTECH OFFICER,
MONETARY AUTHORITY OF SINGAPORE

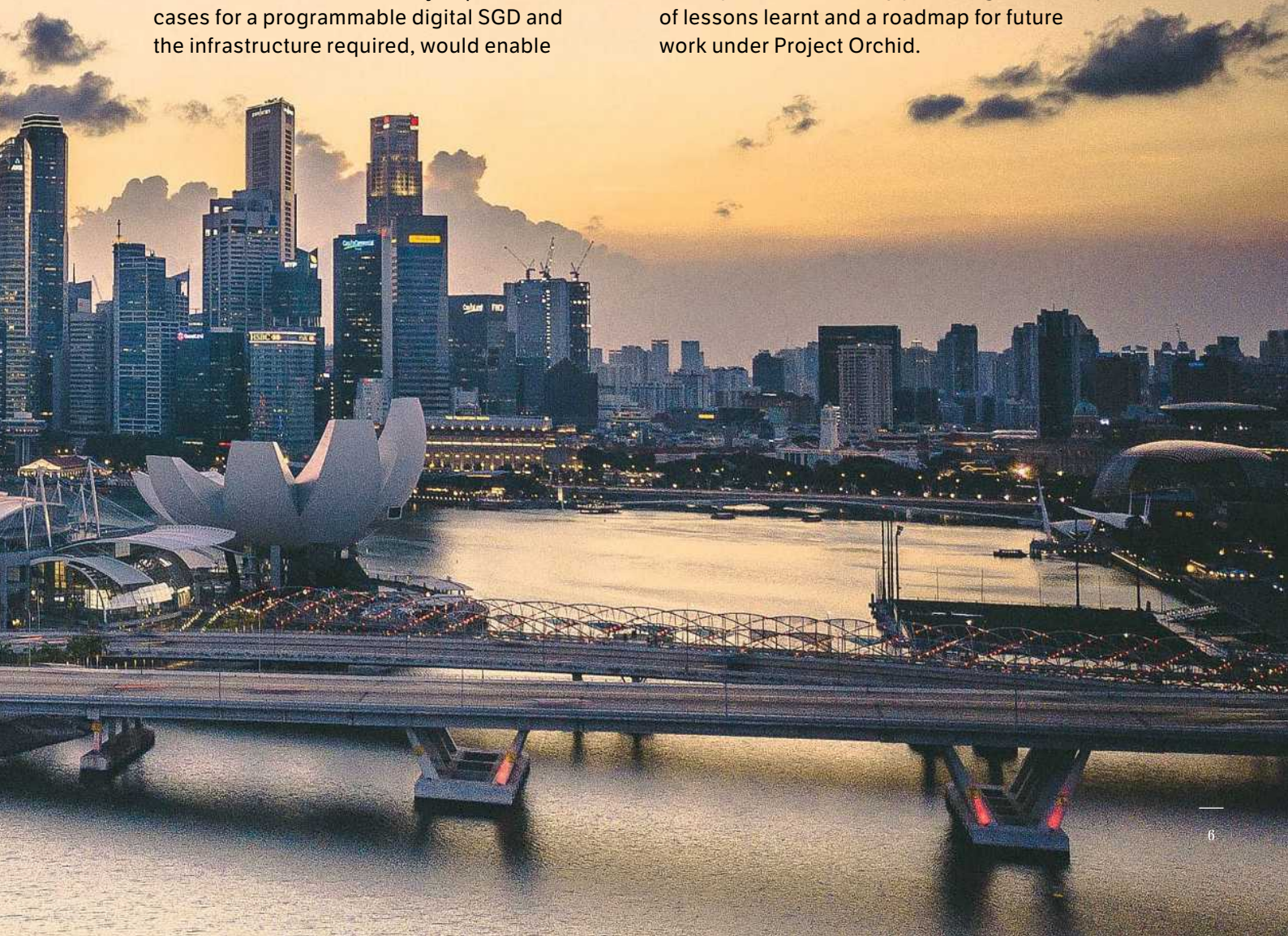
Executive Summary

A potential future digital SGD will need to interact with different forms of digital assets and be interoperable across different financial infrastructures. This report begins with an overview of Project Orchid, the motivation for programmable money and how it supports a digital asset ecosystem. The report introduces the concept of Purpose Bound Money (PBM) and the potential benefits of programmable digital currency through illustrative use cases contributed by industry participants and government agencies.

Central banks, including MAS, would have to assess which combination of financial infrastructure and technology best aligns with its policy goals. An important consideration studied in this report was interoperability with other forms of digital assets through PBM as the common interface layer. Although MAS does not see an urgent case for retail CBDC, it is envisioned that the study of potential use cases for a programmable digital SGD and the infrastructure required, would enable MAS and the financial services ecosystem in Singapore to develop capabilities to support a retail CBDC should the need arises. The subsequent chapters discuss solution approaches for implementing PBM through a common interface and how it might work with various underlying medium of exchanges, mainly CBDCs, tokenised deposits and stablecoins.

The report discusses the design considerations for implementing PBM and features four case studies based on ongoing trials that have been initiated to support the experiments of PBM and a digital SGD. The trials studied the feasibility of public blockchain and their equivalent private implementations, though their inclusion is for experimental purposes only, and should not be inferred as an endorsement on their suitability as financial market infrastructures.

The report concludes by providing a summary of lessons learnt and a roadmap for future work under Project Orchid.



1 — Project Orchid Introduction

Since 1967, Singapore has designed and issued its own national currency. The first Singapore dollar notes circulated were known as the Orchid Series, for the spray of orchids featured in the centre of the front of each note.

MAS has actively experimented with central bank digital currencies (CBDCs) and distributed ledger technologies (DLT) in collaboration with the financial industry and other central banks, beginning with Project Ubin in 2016. MAS' experiments to-date have primarily focused on wholesale cross-border transactions involving financial institutions, in recognition of their potential to address longstanding and emerging challenges in payments.

Project Orchid, launched at the Singapore FinTech Festival (SFF) 2021, marks the first extension of these experiments into the domestic retail payment space (see fig 1). The overarching objective of Project Orchid is to build the foundational technology infrastructure and technical competencies necessary to issue a retail CBDC (i.e., a digital version of Singapore dollar cash), should Singapore decide to do so in the future.

- MAS has assessed[1] that there is no urgent need for a retail CBDC in Singapore at this point in time.[2] The use cases for a retail CBDC are unclear, given that electronic payments in Singapore are pervasive, and households and firms in Singapore are already able to transact digitally in a fast, secure and seamless manner today.
- However, MAS has not ruled out the introduction of a retail CBDC at some stage in the future, in light of the dynamic nature of the payment landscape, evolving consumer preferences and likely growth of the digital asset ecosystem.[3] The case for a retail CBDC in Singapore could strengthen over time, especially if innovative uses emerge or there are signs that digital currencies not denominated in SGD are gaining traction as a medium of exchange locally.

Project Orchid is intended to be a multi-year, multi-phase exploratory project examining the various design and technical aspects pertinent to a retail CBDC system for Singapore, from its functionalities to its interaction with existing payment infrastructures. Project Orchid will build on the learnings from the Global CBDC Challenge organised by MAS and its global partners in 2021.[4]

In its first phase, MAS has partnered the public and private sectors to investigate the possibilities around programmability of a digital currency. For the purposes of this paper, tokenised deposits stablecoins and CBDCs are referred to as digital currency. Programmability is a key enabler of some of the commonly cited use cases for a retail CBDC, even as it is neither an inherent nor unique feature of a retail CBDC. A programmable retail CBDC, together with a set of well-designed smart contracts, could facilitate more efficient disbursement of highly targeted or in-kind fiscal support (e.g., tourism vouchers) and support new business and operating models (e.g., seamless machine-to-machine transactions).

[1] https://www.mas.gov.sg/-/media/MAS/EPG/Monographs-or-Information-Paper/A-retail-CBDC---Economic-Considerations-in-the-Singapore-Context.pdf
[2] **Monetary Authority of Singapore (2021)**, *A Retail Central Bank Digital Currency: Economic Considerations in the Singapore Context, November.*
[3] A digital asset is anything of value whose ownership is represented in a digital or computerized form. It could be a financial asset like a bond, a real asset like artwork, or even an intangible item like computing resources. Digital assets are typically deployed on distributed ledgers that record the ownership and transfer of ownership of these assets.
[4] The Global CBDC Challenge is organised by MAS, in partnership with IMF, World Bank, ADB, UNCDF, UNHCR, UNDP and OECD, that seeks innovative retail CBDC solutions to enhance payment efficiencies and promote financial inclusion.

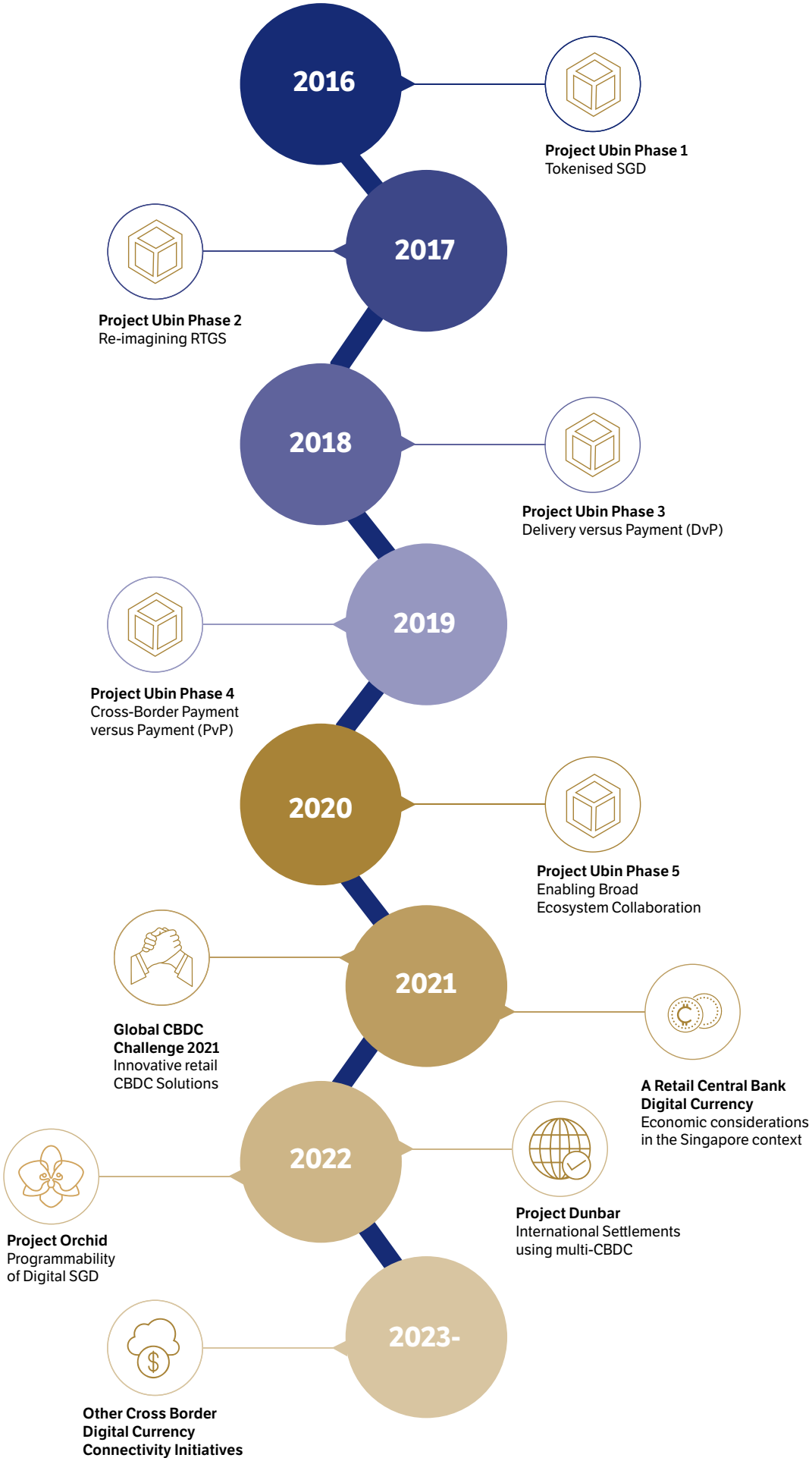


Figure 1: Digital Currency Initiatives

2 — Motivation

Foundational digital infrastructure which supports digital identity, data exchange, and interoperable payments, play an important role in enabling financial services to be accessed by a wider set of the population and support economic and social development. Businesses and innovators could build upon these foundational infrastructures to develop innovative services, leading to more efficient and affordable services with better user experiences. One area where significant strides have been made in recent years is the development of the concept of programmable payment and more recently programmable money popularised with the blockchain and peer to peer money movement.

Programmable payment 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. Today, programmable payments are commonly implemented through setting up database triggers or in the form of Application Programming Interface (API) gateways that sits 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 refers to the possibility of embedding rules within the medium of exchange itself that defines or constraints its usage. For example, rules could be defined such that the medium of exchange could be denominated in fractional units of up to eighteenth decimal places. Programmable money implementations include tokenised deposits, stablecoins 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 it 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 transferrable on a peer-to-peer basis between parties. A third model – **Purpose Bound Money (PBM)**, which is explored in the initial phase of 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 currency can be used. PBMs are bearer instruments, with self-contained programming logic and transferrable between two parties without intermediaries.

A crucial aspect of PBM is that the underlying digital medium of exchange bound within it comes embedded with programmable logic that makes it possible for use across different platforms and systems.

PBMs could be used to digitalise vouchers. 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 gift voucher and transfer it to another person who may then use it at a participating merchant. Vouchers could also be issued to support government disbursement programmes. For example, Community Development Council (CDC) vouchers[5], as part of the Household Support Package in Singapore, are designed to defray the cost of living and support hawkers and heartland merchants affected by the pandemic. The vouchers are distributed to eligible household and programmed to be spent at merchants in the heartlands.

PBM serves as digital bearer instrument, and could in effect support government payouts, Conceptually, the holder of the PBM could present the PBM and cash out without requiring its holder having to have a bank account.

[5] https://www.mof.gov.sg/news-publications/press-releases/1.5-billion-support-package-to-provide-targeted-relief-for-lower-income-households-and-vulnerable-groups

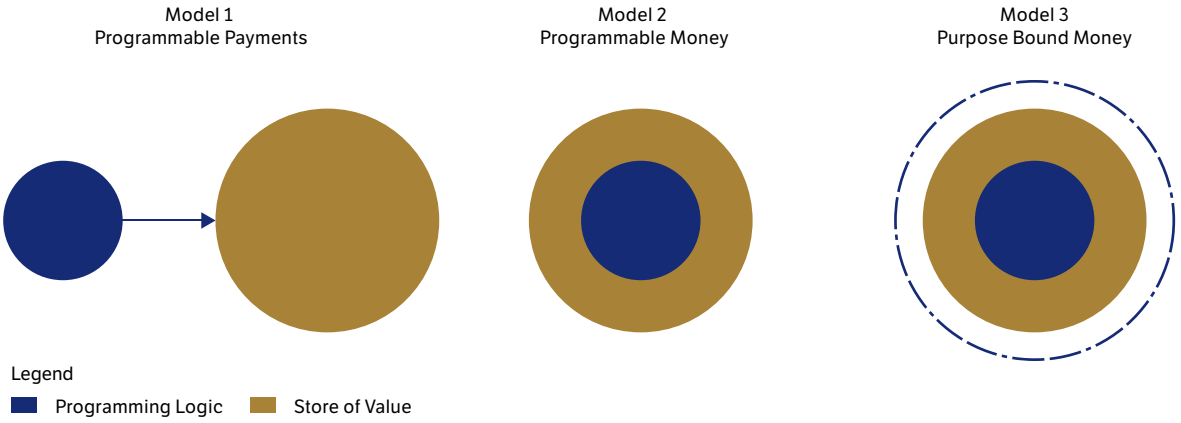


Figure 2: Possible models of programmable digital currency

Proliferation of Schemes

The proliferation of schemes and platforms, increases the complexity and the challenge users face. Voucher schemes today often operate on separate distribution channels with distinct features for different schemes. For example, CDC vouchers are claimed through the RedeemSG[6] system, and digital Grab vouchers are redeemed via the Grab mobile application. Participating merchants would have to train their retail staff to be able to handle and accept different vouchers. This could be onerous, and there could be mistakes made due to unfamiliarity.

Private, independent efforts to consolidate vouchers into a single platform seek to streamline the user experience. To realise the potential of digitalisation, these efforts need to go further to ensure it is open and interoperability across voucher schemes. It should not limit interoperability and access to only consumers and merchants who are subscribed to their platform. Interoperable vouchers and payments systems will allow greater flexibility and provide seamless payment experience for businesses and consumers alike.

Deviation from intended purposes

The risks of misappropriation and deviation from purposes specified in a voucher's terms and conditions is a persistent concern. For example, with direct pay-outs to a person's bank account or the use of cheques, it is not possible for the sender to direct that the recipients spend it at approved merchants and not on vices.

Administrative overhead

Campaign organisers need to typically figure out a host of administrative issues. They would need to figure out operations - e.g. distribution of vouchers across different channels, tracking voucher redemptions, troubleshooting disputes. Currently, even though merchants may have been onboarded to a particular system (e.g. onboarded to the RedeemSG system), they would still need to sign a contract with campaign organisers to agree to accept vouchers for each new campaign it supports.

In addition, under existing voucher schemes, participating merchants do not receive funds immediately. After submitting a claim to the voucher issuer and waiting for days or weeks, the sum is validated and the amount is credited to the merchants' bank accounts.

PBM defines a common interface layer that can be used between different payment service providers, merchants and end consumers to interact with one another without expensive or proprietary 3rd party equipment or institutions to receive payments, nor do they have to build bilateral networks unique only to the parties involved in the transaction. Providers could build upon the PBM standard to foster innovation while still ensuring compatibility with various devices and a collaborative financial ecosystem.

The introduction of PBM could facilitate grant disbursements and mitigate fraud and misuse by embedding intrinsic conditions which govern the use of the underlying digital currencies. Other examples of the usage patterns of PBM are discussed in Section 4 of this report.

[6] **RedeemSG** is a voucher system that helps Singapore Government agencies easily create, issue and track the redemption of vouchers. It also enables merchants to easily accept Government issued vouchers.


MAS
Monetary Auth
of Singapore

3 — Purpose-Bound Money Overview

The concepts covered in this section serve as the basis for discussing the functionalities of PBM, their benefits and risks and investigate how they could be supported by different underlying digital currencies across different real world use cases.

3.1 PBM Architecture

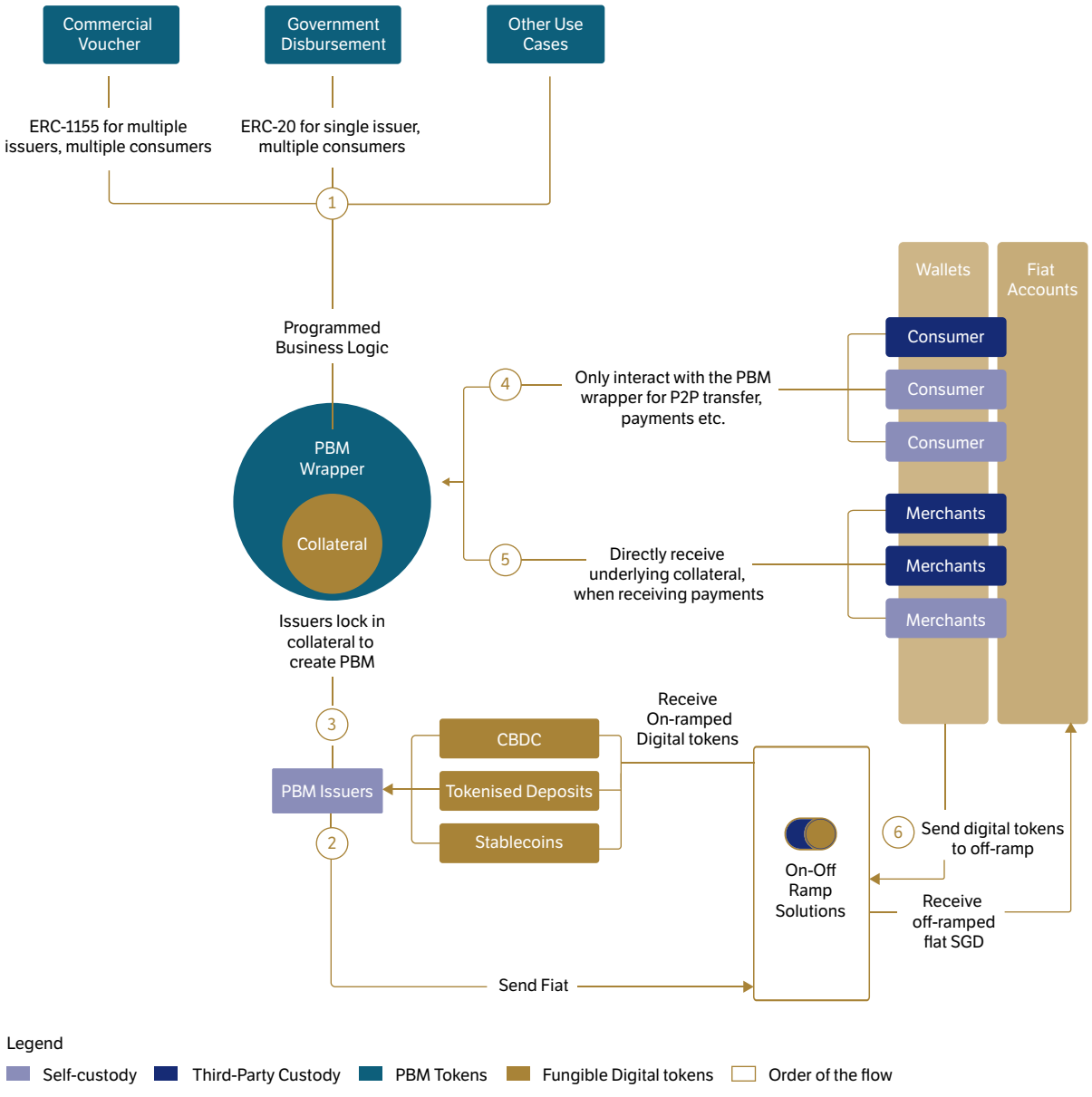


Figure 3: PBM Architecture Diagram

A PBM based architecture has four distinct components.

1. Digital currency backing PBM

The digital currency backing a PBM serves as collateral for the PBM. When the conditions of a PBM are fulfilled, the underlying digital currency is released, and ownership is transferred to the target recipient. To be utilised as a backing digital currency, a digital asset needs to be a good store of value, unit of account and a medium of exchange. Backing digital currencies could come in the form of CBDCs, tokenised deposits or stablecoins that are properly regulated in a manner that provides confidence in the stability of their value (herein known as "securely backed stablecoins"). Backing digital currencies could be implemented as an ERC-20 fungible token smart contract.

2. PBM Wrapper

The PBM Wrapper implemented in the form of smart contract code specifies the conditions upon which an underlying digital currency 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 backing digital currency will be released, and transferred to the recipient. For example, the purpose layer could be implemented as an ERC 1155 Semi-Fungible Token smart contract.[7]

3. PBM Infrastructure

The ownership of a digital currency and the smart contracts governing its usage are executed upon a ledger-based infrastructure. The PBM infrastructure establishes the foundation for the implementation of Programmable Money and enables new possibilities for interactions among consumers, merchants, financial institutions, and government agencies. The ledger-based infrastructure could be DLT or non-DLT based.

4. PBM Wallet

PBM wallets are used by users to send and receive PBMs and the respective backing digital currencies. They refer to cryptographic wallets which are software programmes that hold users' private keys that grants them access to PBMs.

3.2 Digital Currencies backing PBM

In addition to a retail CBDC, PBM technology is also designed to work with other promising forms of digital currencies that could circulate as programmable "money" in the future, namely tokenised deposits and "securely backed" stablecoins.

Any form of electronic or digital money can be considered in two parts: the monetary instrument itself and the supporting infrastructure that allows balances to be managed and transferred. While the starting point is a retail CBDC, the PBM technology has been designed to be

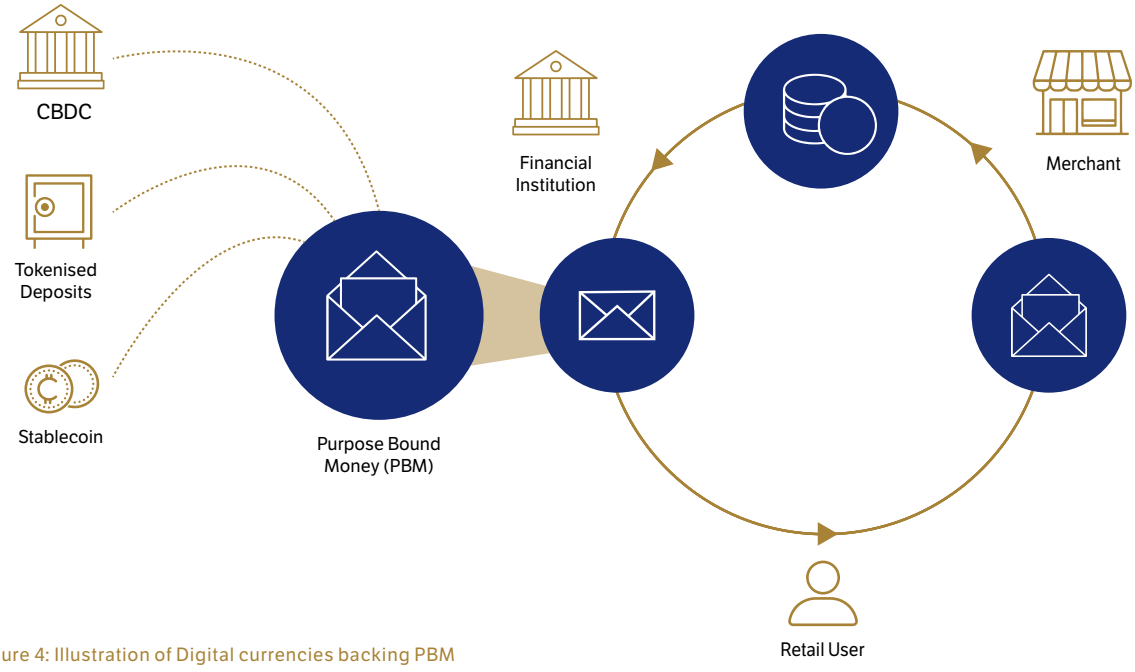


Figure 4: Illustration of Digital currencies backing PBM

[7] Ethereum Request for Comments (ERC) are specifications for Ethereum applications, such as token standards, name registries, library formats, and package formats. ERC-1155 is a token standard that enables the efficient transfer of fungible and non-fungible tokens in a single transaction.

The inclusion of emerging forms of digital currencies in the design of the PBM is solely for experimental and exploratory purposes based on technical grounds and in recognition of the potential they may present.

agnostic to the type of liability underlying it. Three considerations underpin this design choice:

First, MAS expects that, as a monetary instrument, any future retail CBDC will only form a small part of our money supply, playing a useful but ultimately constrained role in the economy just like physical cash. Today, banknotes and coins issued by MAS only account for around 8% of our entire money supply, with privately issued money in the form of bank deposits making up the remaining 92%.

Second, the retail CBDC system will form part of Singapore's national foundational digital infrastructure, which brings together payments, digital identity and data exchange and authorisation and consent mechanisms to protect the privacy and welfare of individuals more holistically. As a public payment rail, it is expected to play an important role in ensuring that the minimum standards required of payments (e.g., in terms of safety, speed, convenience and fees) are present. MAS thus envisages the retail CBDC system to be a common and open back-end platform that is fully interoperable with other existing payment systems.

Lastly, and to a smaller extent, MAS is mindful that the case for a retail CBDC in Singapore remains open at this point. The rapid pace at which innovations are unfolding globally also means that it is still too early at this point in time to tell how the future of money and payments will ultimately pan out. Against these uncertainties, it is MAS' hope that in the process of building up the necessary technical capabilities to issue a retail CBDC, MAS is able to contribute to the common pool of knowledge that will be used to advance the state of payments, regardless of our eventual decision. These reasons suggest that for the PBM technology to be "future-ready" and in line with MAS' vision, it should ideally be compatible with other emerging forms of digital currencies that could potentially circulate as "money" in the future (i.e., a medium of exchange widely accepted for payment of goods and services in the real economy, a stable store of value, and a unit of account). Based on current developments, possible candidates (with varying degrees of likelihood) are synthetic CBDCs, tokenised deposits and "securely backed" stablecoins. Cryptocurrencies (e.g., bitcoin) and other forms of stablecoins (e.g., commodity-backed or unbacked and which adopt an algorithmic mechanism to maintain stability) – based on their characteristics today – are unlikely to have potential to be circulated as "money".

Account-based models typically supports programmable payments while token-based models such as CBDCs and tokenised deposits are Programmable Money with rules embedded within the money itself. PBM wraps the Programmable Money with conditions that will expire once they have been met. Under the initial phase of Project Orchid, participating financial institutions and government agencies tested PBM with tokenised deposit or an existing SGD-denominated stablecoin.

Future phases of the project may include testing with an MAS issued CBDC. The inclusion of emerging forms of digital currencies in the design of the PBM is solely for experimental and exploratory purposes based on technical grounds and in recognition of the potential they may present. For editorial purposes, CBDCs, tokenised deposits and securely backed stablecoins issued by regulated financial institutions, which are denominated in SGD, are collectively referred to as "Digital SGD" in this report.

3.3 PBM Wrapper

PBM can be created from the distinct types of digital currencies, highlighted in the earlier section, through wrapping these digital

currencies in the PBM smart contract. After the PBM has been created, it is distributed to the consumers. Consumers will only interact with PBM in its wrapped form, and they do not have to manage or handle the underlying digital currency. Consequently, there is no need for voucher issuers to issue their own payment instrument. Essentially, PBM Creators are not issuing new payment instruments as PBMs attach conditions to existing payment instruments.

An analysis of the use cases presented by the PBM working group suggests that a PBM undergoes similar lifecycle stages, regardless of its underlying technical implementation. Consequently, there is merit in developing an open, standards-based interface specification that will serve as a common framework for future PBM development work. The provision of the interface specification through an open-source software project will further encourage adoption and enable greater interoperability across participating systems.

3.4 PBM Infrastructure

The PBM solution is designed to work with both DLT and non-DLT based ledger infrastructure.

Among DLT based infrastructures, public and permissionless blockchain networks provide the digital infrastructure to support peer to peer transactions at a large scale globally. Applications which are deployed on these networks, can sometimes reach millions of users immediately without having to be concerned about onboarding them individually. Public blockchains however have their own set of trade-offs, such as the lack of clarity on accountability in the event of a catastrophic failure or clarity on who are the entities running the nodes. There is also no definitive service level agreement, which makes it challenging for it to be adopted as a financial market infrastructure. Additionally, the transaction fees needed to incentivise validators to keep the network secure may become exorbitant on popular networks and limit scalability.

Meanwhile, private and permissioned blockchain and other distributed ledger-based networks using technologies such as Hyperledger Besu and Corda provide better clarity on the parties accountable for running the network. However, these networks tend to be smaller in size, relative to the scale which public blockchain networks have been able to attain.

Aside from blockchain based solutions, digital currency projects are exploring the use of centralised ledgers which adopt similar data structure as blockchain networks but without the need for decentralised operations. An example is the OpenCBDC[8] ledger initiative by MIT in collaboration with the Boston Fed.

The experiments conducted under the initial phase of Project Orchid examines the interoperability of PBM across different types of ledgers – both public and permissioned as well as centralised and decentralised. The inclusion of public and private blockchains are solely for experimental and exploratory purposes based on technical grounds. It does not constitute an endorsement by MAS of them as being suitable as financial market infrastructure. The design and selection of an optimal ledger for a retail CBDC is a potential topic for research in future phases of Project Orchid.

3.5 PBM Wallets

PBM is designed to be compatible with common cold and hot cryptographic wallets which stores a user's private keys. These wallets could be provided by commercial or government entities. The wallets need to factor in additional risks in terms of accidental loss, who conducts the transactions, and how transactions are monitored and recorded. While some retail users may prefer to have complete control over their digital assets via self-custodial wallets, others prefer them to be held under the custody of an institution for accountability and insurance. The institutional setup of self-custody may require expensive hardware (e.g. Hardware Security Modules (HSM)), proper workflow systems and trained personnel to ensure compliant operations.

The next chapter discusses the various interaction patterns associated with the use of PBM within different contexts in the following sections.

[8] **OpenCBDC** is a project maintained by MIT which will serve as a platform for further CBDC research. Project Hamilton, a multi-year collaboration between the Boston Fed and MIT's Digital Currency Initiative, released code that contributed to OpenCBDC project.


Tower

4 — PBM Usage Patterns

This section examines **how a person would use a PBM** under different scenarios. The opportunities for improving interactions between stakeholders are discussed. Section 7: Case Studies provides a more detailed elaboration of how PBM is used in practice and lessons learnt till date.

Use Case	Interaction Patterns (Transfer of value)	
GOVERNMENT	**Government to Person**	**Person to Government**
	E.g. Government Disbursement	E.g. Pay Taxes
COMMERCIAL	**Corporate to Person**	**Person to Corporate**
	E.g. Corporate Vouchers, rewards points	E.g. Commit to spend
INDIVIDUAL	**Person to Person**	
	E.g. School Allowance, purpose bound donation	

4.1 Government to Person

Background

Governments provide various types of fiscal transfers to citizens with the intention of supporting a target segment of the population or stimulating the local economy. Government disbursement programmes target different stakeholders and are designed to achieve multiple social objectives. Consequently, each programme may have different characteristics.

For example, in Singapore, CDC vouchers, which are designed to uplift the economy during the COVID downturn particularly for heartland merchants and to inspire the unity of Singaporeans during the pandemic, are set to be spent within a certain amount of time. Another initiative is the Climate Friendly Household programme where vouchers that are issued can only be used at participating merchants for energy efficient light bulbs and other climate friendly electrical appliances.

Open Government Products (OGP)[9] built a Government Voucher system "RedeemSG" that helps Government agencies to easily create and issue digital vouchers, whilst also providing them with transaction reports to ease financial reconciliation. It also allows participating merchants to easily accept Government issued vouchers. The system is estimated to issue S$800M worth of voucher campaigns across various government agencies, such as the aforementioned CDC vouchers and Singapore's National Environment Agency (NEA) vouchers. To date, more than 2.33 million sets of vouchers have been issued to citizens with a total transaction value of $192.7 million directed back at local merchants. More than 96% of Singaporean households have claimed CDC Tranche 1 vouchers supported by RedeemSG.

Another solution is GovWallet that supports the distribution of pay-outs from agencies to beneficiaries. Agencies can manage their distribution programmes while beneficiaries can track their payout and spending history via the official government apps such as the LifeSG mobile app. From the LifeSG app, beneficiaries can scan the SGQR, NETS or PayNow QR codes to pay the merchants directly. There are more than 164,000 and 43,000 merchants registered with PayNow and NETS respectively today.[10]

Current Challenges

Currently, campaign organisers, such as CDC and NEA, need to work out a host of implementation details from scratch. For example, they would need

[9] Open Government Products is a division of GovTech Singapore
[10] https://www.developer.tech.gov.sg/products/categories/platform/govwallet/overview.html

to figure out how to disburse the vouchers, and how to reconcile transactions when vouchers are redeemed. As a result, it could take months or in some cases years from the time that a voucher campaign is conceived to the time it is being implemented. The current RedeemSG system reduces the time it takes for a merchant that is already on the RedeemSG system, to be onboarded to new voucher campaigns. However, a participating merchant still needs to sign separate contracts with the respective campaign organisers before taking part in the campaign.

Implementation cost

Several campaign organisers have taken to commissioning their own voucher system to be able to meet their objectives. These custom systems, based on anecdotes, could cost campaign organisers thousands or millions to build.

Settlement processing time

To process a claim on a voucher, the campaign organisers, merchants, the banks of voucher issuers and the merchants' banks, all need to ensure that the net cash flow amongst all parties is accurate and correct. The reconciliation process includes the following:

- The campaign organiser needs to ensure that the amount paid to the merchants is equal to the amount of vouchers collected back from the merchants.
- The merchants need to ensure the amount received from the voucher issuer is equal to the amount of vouchers they collected from the residents.
- The voucher issuer's bank needs to ensure that the cash settlement from their bank to all the merchants' banks are accurate.
- Respective voucher issuers need to ensure the cash received from the voucher issuer's bank are accurate.

A reconciliation mismatch between any party would lead to a long and costly dispute resolution process.

Fraudulent Claims and Exploitation of Government Social Programmes

Unfortunately, scammers have targeted government payouts, defrauding agencies by submitting fraudulent claims to receive reimbursements by the government. Some syndicates have gone further, falsifying documents such as employment contracts and attendance at training courses, which were never conducted.

Solution Overview

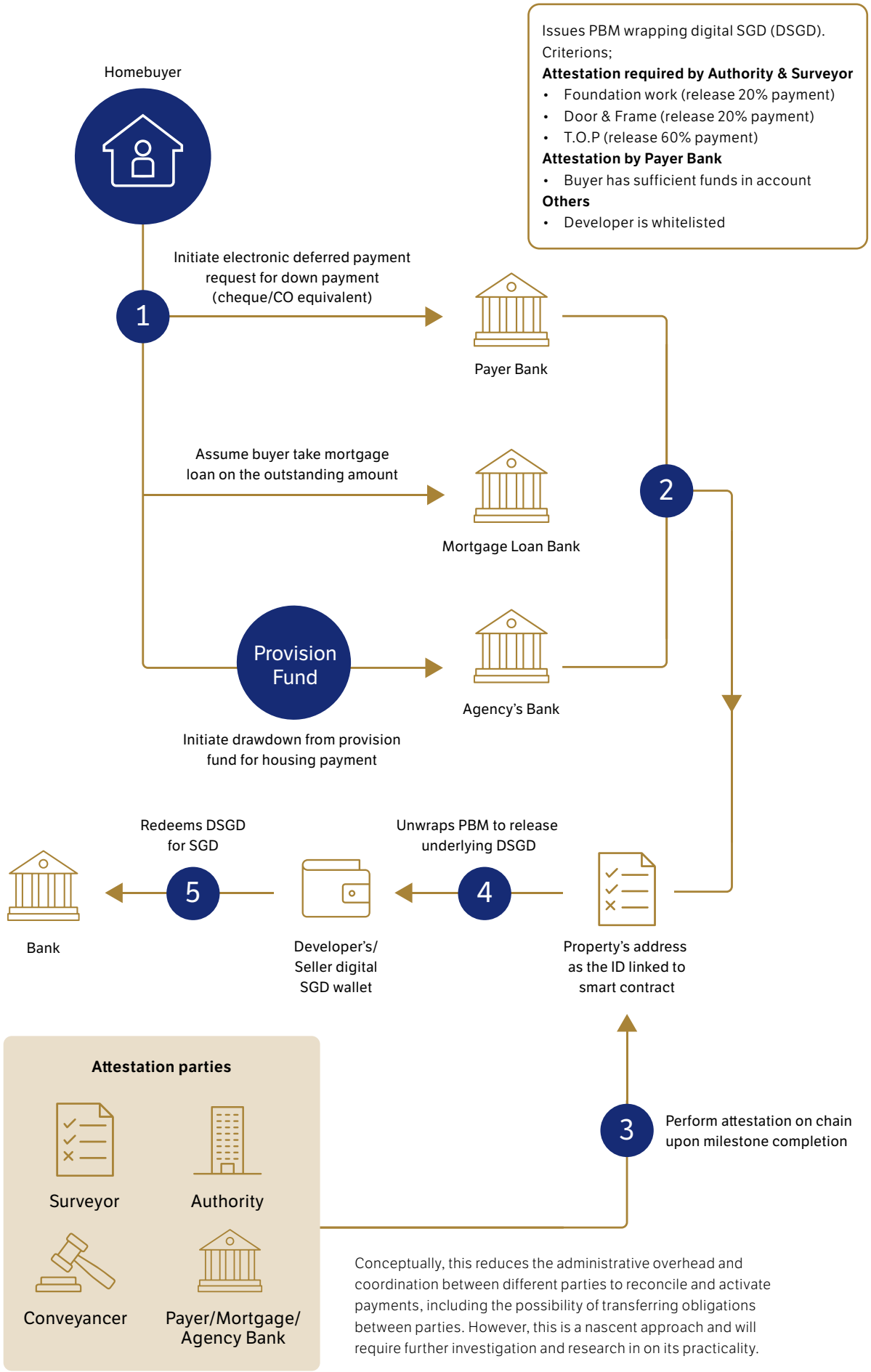
The programmability feature of PBM allows government agencies to have greater flexibility in defining conditions for how and where the funds distributed could be used. This supports the delivery of more targeted social assistance. To ensure that citizens are spending their digital vouchers based on the intended fiscal transfer objectives, spending conditions can be set accordingly. These conditions could be:

- recipients receiving different amounts based on household income or housing type
- spending only at specific merchant categories (e.g. supermarkets or shops outside the city centre)
- specific voucher features (e.g. expiry dates, etc.)
- other terms and conditions of these digital vouchers that can be defined in the PBM smart contract and validated programmatically during the transaction to ensure that all parties fulfil their obligations.

Potential solution flow:

1. Government agencies specify the terms and conditions for where and how digital vouchers should be used. Based on the conditions specified, a PBM is created based on an underlying digital currency and distributed to eligible citizens.
    a. Traditional fiat currency is transferred from the government agency to the digital SGD issuer
    b. The digital SGD issuer mints the digital SGD for the government agency's purpose.
    c. A PBM is created for the government agency's distribution to eligible citizens, businesses for spending at approved institutions.

2. When an eligible citizen shops at eligible merchants, they can use PBMs to complete the purchase after selecting the eligible goods and services. As a consumer, the eligible citizen scans-and-pays with PBM. When the PBM is used, a 3-step evaluation of the smart contract terms is performed.
    a. Verifies that the PBM is valid (e.g. institution is approved, within validity period, sufficient balance)
    b. Checks if obligations are met (e.g. proof of attendance, proof of goods delivered)



Conceptually, this reduces the administrative overhead and coordination between different parties to reconcile and activate payments, including the possibility of transferring obligations between parties. However, this is a nascent approach and will require further investigation and research in on its practicality.

Figure 5: Illustration of PBM in context of Property Stamp Duty Payment

c. Redemption amount expected – in full or partial payment for goods delivered.

3. Where conditions are met, the underlying digital currency backing the PBM is unlocked and the funds released to the merchants.

Potential Benefits of PBM

PBM could complement existing government platforms such as GovWallet and RedeemSG. Currently, these platforms provide the ability to specify and distribute PBM to targeted groups (Model 1). PBM extends existing capabilities by providing the option to specify conditions that need to be met before the money is released, (Model 3). These conditions are embedded within the voucher scheme itself, such that the conditions for use are transferable when the vouchers are exchanged. This expands the tools that policymakers have in their toolkit to improve the efficacy of government social programmes.

Ease of Onboarding Merchants

PBM supports a more programmatic mechanism for targeting groups of merchants participating in a campaign. Merchants that are already onboarded to the platform would be able to support a new voucher campaign easily. As the conditions are defined by the PBM Creator and enforced through smart contracts, there is no additional effort for merchants. The merchants receive digital SGD and not the vouchers, hence the programming logic specified by the PBM Creator is transparent to them. Unlike existing mechanisms, PBM Creators do not need to sign contracts with individual merchants for each new voucher scheme. Consequently, this is more scalable than existing infrastructures.

Transparency

PBM smart contracts, if deployed onto public ledgers, offer greater transparency for government social programmes. For example, the total amount of digital vouchers created by campaign organisers could be visible and the flow of PBM from government agencies to citizens and to merchants could be traced. Nonetheless, increased transparency needs to be balanced against other policy goals such as personal data protection policies.

Transferability

Like a physical voucher, the transfer of PBM tokens amongst merchants and recipients can be facilitated without requiring a central coordinating party. This makes it possible to cater to the unique operational needs of programmes. Furthermore, if the PBM was not used within its validity period, the underlying digital currency backing the PBM could be "released" back to the government agencies who funded the programme and recycled for future use.

Some programmes might wish to enable citizens to transfer their vouchers amongst one another easily, efficiently, securely, and safely. For example:

- Campaign(s) like SingaporeRediscover vouchers that want to allow recipients to choose to donate their voucher to charities/ needy individuals
- Heartland Pays It Forward programme in which recipients can "pre-purchase" meals for needy individuals
- Campaign(s) in which each recipient's spending would dynamically trigger the issuance of a voucher to incentivise more spending at a particular Government-owned shop

4.2 Person to Government

Value transfers could occur in the opposite direction, whereby a person could initiate payment to a government agency. One example of such a flow is buyer stamp duty payment to tax authorities or payment for property purchases to housing agencies. In these examples, there is a possibility for PBM to be used to model the obligation to pay upon completion of milestones.

Potential solution flow:

1. When a homebuyer initiates an application to buy a property, there are different milestone events upon which payments need to be made. For example, a portion of funds is released upon foundation work being completed or obtaining a Temporary Occupation Permit (TOP).[11] A PBM could be created based on terms stipulated with the sale of the property.
2. 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.
3. Attestation parties such as surveyors,

[11] A Temporary Occupation Permit (TOP) is the permit from the Building and Construction Authority (BCA) to allow building owners to occupy the premises when key works have been satisfactorily completed and certified by the other authorities in Singapore.

conveyancing firms, and banks provide their confirmation when milestones have been completed.

4. The smart contract checks that the milestones have been completed based on the attestation provided. Upon milestone completion, the PBM is unwrapped and the corresponding funds could be released to the seller or a property developer. Conversely, if the developer fails to meet any of the milestones on time, PBM could be programmed to deduct compensation or penalties based on predefined formula.
5. The developer or seller who are in receipt of the digital SGD could use it for their next transaction or convert it back to traditional fiat currency through a deposit account held with a bank.

Potential Benefits of PBM

Reduce administrative overhead

PBM enables payments to be automated. With the use of PBM, the settlement processes could be streamlined and more efficient. The consumers are protected, as the funds are released only upon completion of work.

Tracking progress of payments

An extended benefit is that payment could be setup to align with the the delivery of the individual project milestones. possibility of tracking the alignment of payment and delivery through a common view is possible. For example, for payments of property purchases, homebuyers could track their alignment with the milestones of the property's development. These milestones could include the setting up of electrical sockets and lights, the painting and flooring of the property and the movement of furniture into the property.

4.3 Corporation to Person

Background

The flow of value could also occur from corporations to individual persons in the form of corporate vouchers and platform-specific rewards points. In this flow, a corporate could be from non-finance industries, such as lifestyle, entertainment, medical, food and beverage.

Current Challenges

Today, a popular mechanism for corporates to distribute rewards or to direct spending is the use of physical vouchers. The process of issuing, distributing, and redeeming vouchers could be onerous and vulnerable to loss during transit.

In addition, campaign organisers would need to tally and account for the use of vouchers before reimbursing participating merchants. After tabulating, they would periodically settle the amount owed to merchants for a particular time period (e.g. a day to a month). This results in a longer time lag before merchants get paid.

Moreover, corporations typically offer commercial vouchers through their own proprietary platforms. Hence, users holding multiple vouchers would have to navigate across different mobile applications and websites, remembering the terms and conditions for using each of these vouchers as they do so.

Solution Overview

PBMs could be used to mitigate some of the challenges currently faced when transferring value from a corporation to a person.

Potential solution flow:

1. Corporates offer shopping, grocery and travel vouchers to consumers in the form of PBM
2. Consumer receives the PBM via their mobile banking application
3. Consumer scans-and-pays with PBM.
4. Merchant accepts the PBM as a form of payment. Digital SGD is transferred into the merchant Wallet.
5. Merchant delivers the goods or services.
6. Only upon completion of conditions (e.g. goods and services delivered by the merchant), Merchant is allowed to drawdown funds in their wallet.

Potential Benefits of PBM

Interoperability

PBM enables the widespread distribution of programmable money in the commercial world. Interoperability with e-wallets and payment networks, will enable PBM to be distributed widely across different platforms. Consumers could therefore use PBMs to offset payments or redeem for goods and services through a multitude of platforms with their own preferred digital wallet. There is no need for voucher issuers to issue their own payment instrument. Essentially, PBM Creators are not issuing new payment instruments as PBMs attach conditions to existing fund transfers.

Enhanced Merchant and User Experience

The use of PBM might enable a more user centric experience, whereby a consumer could access PBMs from different corporates and schemes from their preferred wallet application. Consumers would also be able to keep track of the different vouchers they have through a single application, instead of across multiple different applications, if they prefer to. With increased visibility, this increases the opportunity to direct or affect user behaviour at the point of purchase. In terms of consumer targeting, merchants will be able to achieve commercial, social, and marketing objectives through specifying PBM conditions that are designed for certain scenarios or specific consumers.

Validity check

Another positive feature of PBM is the ability to validate the payment instrument automatically. When consumers use PBM for retail purchases, a validation check happens in the smart contract during the transaction process to ensure that all the conditions specified in the PBM are met before the transaction can occur. Therefore, merchants do not need to manually check each digital voucher to ensure that it fulfils campaign conditions. This greatly improves the efficiency of payment processes via the use of PBM.

Real time settlement

With PBM, the moment a consumer uses a PBM for payment, the PBM token will be unwrapped, thereby releasing the underlying digital currency and transferring it to the merchant's digital wallet. This digital currency can then be used by the recipient immediately to fulfil any of their personal financial needs.

4.4 Person to Corporation

Background

The transfer of value could also occur from individual persons to corporations. This could be scenarios whereby consumers are required to pay upfront before the service is delivered. Gyms, fitness studios, nail salons, tuition centres, travel agencies are examples of businesses which collect some form of prepayment from consumers before the delivery of good and services. Amounts collected are often substantial as they involve big-ticket items or long-term commitment.

Current Challenges

Consumers stand to lose the deposits they have made upfront, as payments on goods and services for future delivery, if the merchants they were dealing with went out of business. For example, when oBike went into liquidation in 2019, about 220,500 former oBike users were owed S$8.9 million.[12] Another example is California Fitness who shut its outlets island wide in 2016, impacting users who have signed up for their membership packages.[13]

Solution Overview

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 "draw down" 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.

Potential solution flow

1. Consumer funds wallets with digital currencies that can be used to create a PBM .
2. Consumer creates a PBM with conditions of upfront payment.
3. Consumer scans-and-pays with PBM.
4. PBM is accepted and the underlying backing digital currency is transferred into the merchant's wallet.
5. The corporation delivers the service
6. The corporation is only allowed to drawdown funds in the form of the PBM's backing digital currency in their wallet upon completion of conditions (e.g. 3 of 12 months gym membership; 5 of 10 services redeemed).

[12] https://www.todayonline.com/singapore/no-progress-sight-former-obike-users-retrieve-their-deposits-around-s455000-claims-filed
[13] https://www.straitstimes.com/singapore/california-fitness-liquidators-report-closes-door-on-member-refunds-blames-management-and

Potential Benefits of PBM

Enhancing security for Escrow[14] accounts

PBM could be used for payment of services that require upfront payment or bulk purchases. With PBM, the consumer pre-commits to spend a fixed amount of money for the service, giving assurance to the service provider on future revenue while also ensuring consumer's interests are safeguarded by allowing the service provider to draw on the money only when a specified portion of the service is provided (Eg. Spa credits and packages). This could serve as an alternative to setting up escrow accounts.

Providing alternatives for conditional payments

In Singapore, FAST transfer enables immediate fund transfers today between individuals and corporates through their bank accounts. However, it does not provide a facility to allow individuals or corporates to specify what and how their funds would be used for and how long the funds are available to the beneficiary. The use of PBM technology enables individuals or corporates to define and embed logic-based conditions in the form of smart contracts. These smart contracts automatically verify and process the embedded conditions when the PBM is submitted for transfers.

4.5 Person to Person

Background

The distribution of value could occur amongst individuals, whereby the sender may have expectations on how recipients should spend the funds. For example, parents may grant their children allowances, with the intention that they will use the money to purchase books in designated bookstores or for their meals in school but not for other purposes.

Besides student allowances, another example of a targeted Person to Person value transfer is the wish for individuals to send donations to various non-profit organisations for specific purposes.

Current Challenges

Today, potential donors might be inundated with a proliferation of charities and social service organisations that are seeking funds to support their causes. A recurring concern that potential donors have is whether their donations reach their intended beneficiaries, and if the funds are used for their intended purposes.

Furthermore, for overseas beneficiaries, there may be a lack of transparent, secure and economically viable option for remitting the funds, especially to remote areas. They may also be challenged with exorbitant foreign exchange fees imposed onto their donations such that the beneficiaries would ultimately receive a donation thatis a small fraction of the original value donated.

Consequently, potential donors may be hesitant to contribute to social causes because of the information gap that exists between potential donors and beneficiaries.

Solution Overview

PBM for donations are traceable and programmable donations such that beneficiaries could only receive the underlying digital currency when conditions are met.

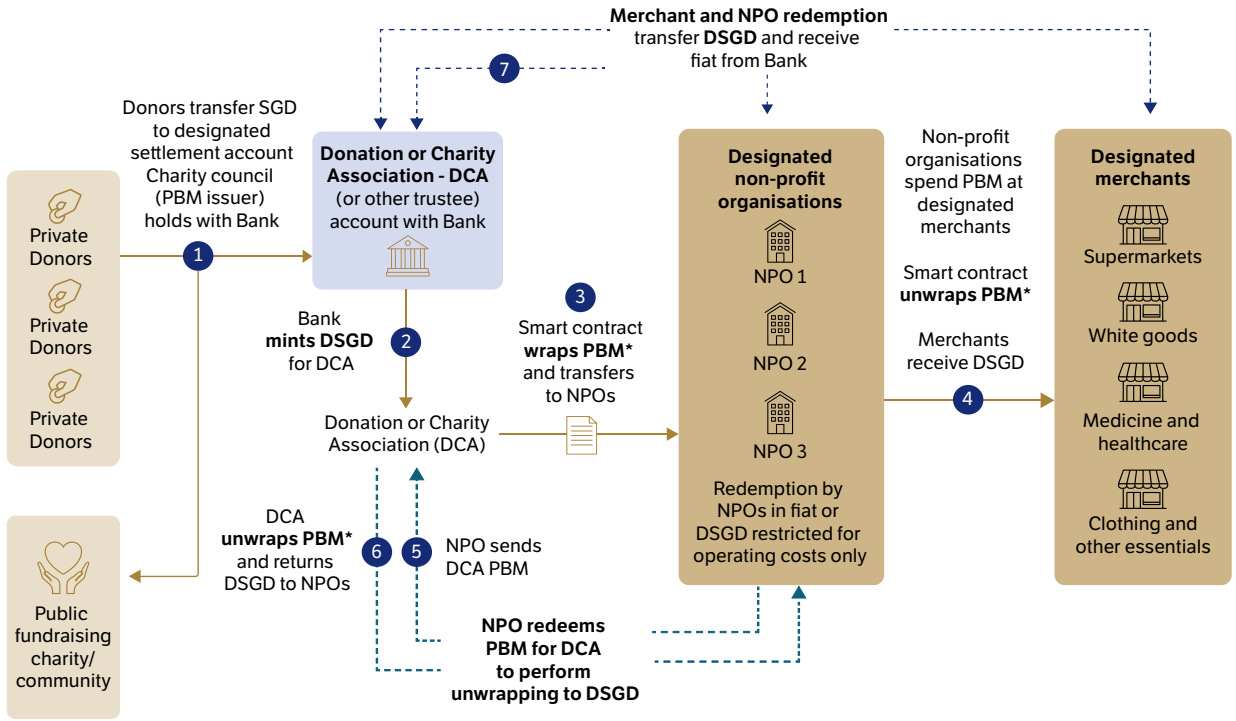
Potential solution flow

1. Individual donors or Charities and Institutions of a Public Character (IPCs), transfer SGD to a designated settlement account (e.g. held with DBS Bank)
2. Digital SGD Issuer mints the digital SGD for the charity association's trustee account with Digital SGD Issuer.
3. The charity association determines the grants received by the non-profit organisation (NPO) under their charge and defines the terms and conditions for which the digital SGD could be used.
4. The NPO, a beneficiary of the PBM, spends the PBM at designated merchants. The designated merchants receive the digital SGD.
5. In the case of unspent PBM, NPOs can redeem for digital SGD from the charity association.

[14] A bond, deed, or other document kept in the custody of a third party and taking effect only when a specified condition has been fulfilled


yummy viet
vietnamese cuisine
ROYAL
28A
ROYAL™
HOSTEL • CHINATOWN
YourSingapore
Free Wi-Fi
免费无线互联网
Log on to
Wireless@Chinatown
Supported by:
Fire Engine
Access
Keep Clear
Beijing Duck
北京烤鸭
Traditional
MASSAGE
22A


FOLKS



*Wrapping/unwrapping of Purpose bound tokens can be undertaken by Bank directly.

Figure 6: Illustration of PBM in context of Donations

Potential Benefits of PBM

Improving Efficacy of Donations

PBM could enable charity organisations to have greater oversight over the spending behaviour of the beneficiary organisations that they administer their grants towards. Grant making organisations could track the PBM and their usage, thereby deriving the effectiveness of their programme as well as support the provision of more transparent reporting to their donors. More donors would be encouraged to come forward if there was greater transparency on how their contributions are used by the non-profits they have donated to and better visibility on the impact it has made.

In addition, restricting the use of PBM to a curated list of participating merchants, ensures fair charging to grant recipients. Further, it guards against fraudulent organisations looking to have a claim on disbursed donation proceeds without an intention to deliver the intended service outcome.

Reducing Fraud

PBM technology could be used to mitigate the unilateral and unauthorised use of funds. Transactions are recorded on an immutable append only ledger with the possibility of aiding investigators with appropriate access to uncover the occurrence of malicious acts such as the modifications of terms of use of a PBM. For PBM Creators, the redemption mechanics and spurious behaviour could be tracked and managed.

5 — PBM Functional Overview

A PBM is envisioned to have common lifecycle stages across different programming languages and network protocols, regardless of its underlying technical implementation. This chapter introduces the expected functionalities of PBM and associated lifecycle stages.

The adoption of a standard PBM framework across industry participant is important to achieve interoperability across relevant systems and touchpoints. The framework should be open and governed by a group of trusted entities across different organisations.

5.1 PBM Lifecycle Stages

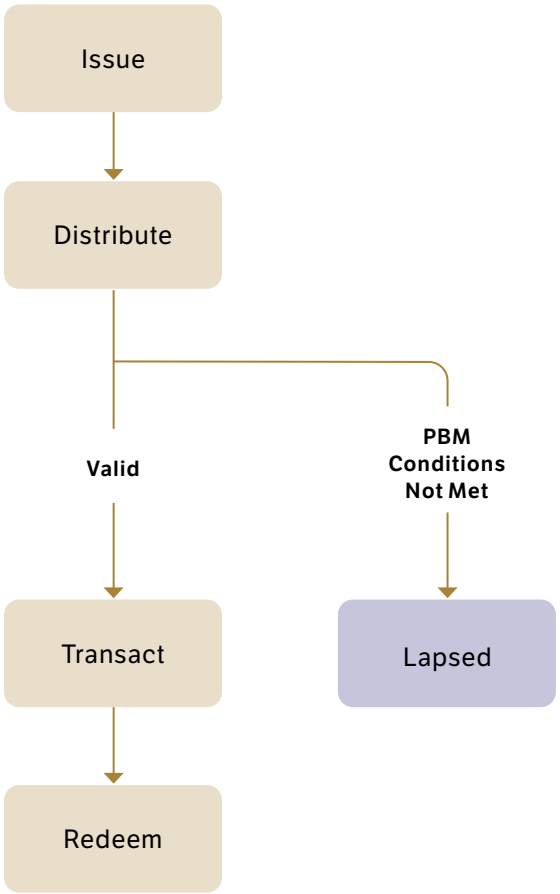


Figure 7: PBM Lifecycle

- **Issue:** This is the point in which a PBM is created. The backing digital currency (e.g. Digital SGD) is bounded by a smart contract (e.g. implemented as an ERC 1155 smart contract or equivalent), and its usage tied to conditions that are specified in the smart contract. The PBM at this stage is created, issued by the PBM Creator, and made publicly available, however, not yet claimed by the consumer.

  Figure 7 provides a detailed elaboration of how PBM is created. First, the PBM Creator sets the terms and conditions for how the PBM is intended to be used. These terms could be parameterised, and the conditions translated to smart contract code. Next, the PBM Creator deposits traditional fiat currencies equivalent to the total value of the PBM with the digital currency issuer. The digital currency issuer, who is a regulated financial institution, mints, and provisions the underlying digital currency backing the PBM. Finally, the PBM is created according to the terms and sent to the issuer for distribution.

- **Distribute:** After a PBM has been issued, it is distributed by the PBM Creator (E.g., corporate voucher sponsor) to consumers for use through publicly available channels (E.g. airdropped to a user based on whitelisted wallet addresses). The PBM Creator may also engage a third party to help with the distribution of the PBM.
- **Transact:** when a valid PBM is acquired and spent by a customer according to the parameters set in the smart contract. As an alternative to spending the PBM, a PBM can be transferred from one person to another person. When a PBM is transferred, the conditions governing its use remain in force. The recipient of the PBM can only utilise the PBM under the conditions specified by the original PBM Creator.
- **Redeem:** this lifecycle stage refers to when participating merchants receive the PBM from consumers. This course of action would trigger an unwrapping of the PBM to redeem the underlying digital currency. The ownership of the digital currency would now be transferred to the merchant's wallet address.
- **Lapse:** when at least one of the conditions set in a PBM's smart contract, such as time

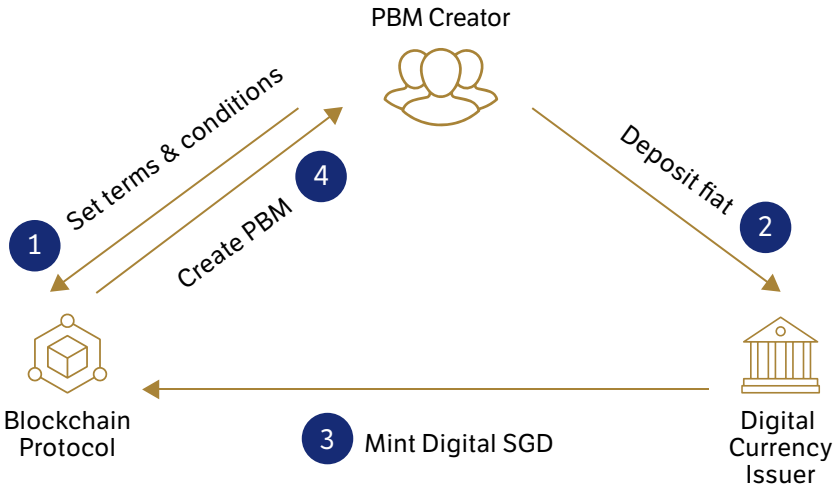


Figure 8: Detailed Process of Issuing PBM

constraint, or designated purpose of spending, is undeniably expired or violated, a PBM is considered lapsed and no longer valid for use. Depending on the preferences and requirements of the PBM Creator, lapsed PBMs can be aggregated and destroyed or "burnt" to return the underlying digital currency and deposited funds to the PBM Creator. The PBM can also be paused for an indefinite amount of time to prevent the public from further interacting with the expired PBM.

5.2 PBM Roles and Responsibilities

In this section, the roles and responsibilities under a PBM based design are introduced. The guiding principle for how they should operate are highlighted.

Role	Responsibilities under PBM based design
REGULATED / LICENSED DIGITAL SGD ISSUER	• As a licensed and regulated institution, the digital issuer will provision Digital SGD to the PBM Creator • Responsible for ensuring promise of stability in their value • Responsible for defining the roles and access control of participants • Responsible for fungibility of the token pegged to the same currency (This will be covered in future phases of Project Orchid)
LAST MILE SETTLEMENT	• Provide the on/off ramp services
WALLET PROVIDER*	• Responsible for onboarding merchants • Responsible for providing wallet management services • Wallet provider will be able to allow their users to access and spend their Digital SGD directly from their app
PBM CREATOR	• Responsible for defining the roles and access control of each member involved in accessing the PBM Token smart contract • Responsible for minting, burning and freezing PBM tokens • Responsible for defining their own PBM token business logic. Eg. Voucher expiry date, approved merchant list, min transaction values • PBM Creators have to earmark their Digital SGD in order to mint PBM tokens • PBM Creators will handle the distribution and management of their PBM tokens • PBM Tokens should be compatible with 3rd party wallet providers
PBM HOLDER	• Responsible for choosing his preferred wallet application to view and spend his PBM token • A Retail User would be able to directly receive all his PBM tokens from various PBM Creators • A Retail User would be able to select a wallet of this choice to manage and spend the PBM tokens from various PBM Creators
PBM REDEEMER	• Responsible for accepting PBM tokens and Digital SGD if they're onboarded to the scheme • Receive Digital SGD once redemption conditions are met

Table 2: Roles and Responsibilities

*Wallet provider could be merchant acquirer or consumer wallet.

5.3 PBM On-ramp & Off-ramp

In this paper, CBDCs, tokenised deposits and securely backed stablecoins are referred to as forms of digital currencies while physical notes, coins and bank deposits as traditional fiat currencies. This section describes the conversion process between traditional fiat currencies and digital currencies.

On-ramp is a term commonly used to refer to the process of enabling users to exchange their traditional fiat currency[15] for digital currency while off-ramp entails the opposite of the process where users can withdraw into traditional fiat currency by converting their holdings of digital currency.

For individuals and corporates who would like to hold and utilise digital SGD for their next transaction, there is no need to go through the process of converting to fiat currency.

On-ramp Experience

For the on-ramp process, the end-users' experience needs to be seamless, while ensuring the integrity of the process is maintained, ideally with minimum manual intervention.

1. Users need to be onboarded and equipped with a compatible PBM wallet before they can proceed. Wallets could be held by the end-user (self-custodial) or held by a financial institution on behalf of a user (custodial).
2. If PBM creators do not have the requisite digital SGD in their wallets, the following steps would be required.
    - PBM Creators, either retail users or corporates, could top-up their bank accounts and make an on-ramp request to convert Fiat (SGD) in their bank account to Digital SGD token in a cryptographic wallet. As banks hold the Current Account Savings Account (CASA) of customers (retail or merchant), the conversion process would happen directly.
    - For non-banks, a request could be made via APIs to enables deposits through standard bank wire instructions and funds received assigned to unique virtual accounts associated with the end-user.
3. Once digital SGD has been set aside, the PBM Creators proceed to specify the conditional logic for the PBM, the PBM is then created with the digital SGD as the collateral backing the PBM
4. End-Users receive the PBMs by providing a compatible wallet address or through a QR code mechanism. The PBMs will be distributed to the users, by sending the tokens to their wallet addresses. A unique identifier, e.g. registration ID or email, is being used to ensure the integrity of the PBM distribution among users.

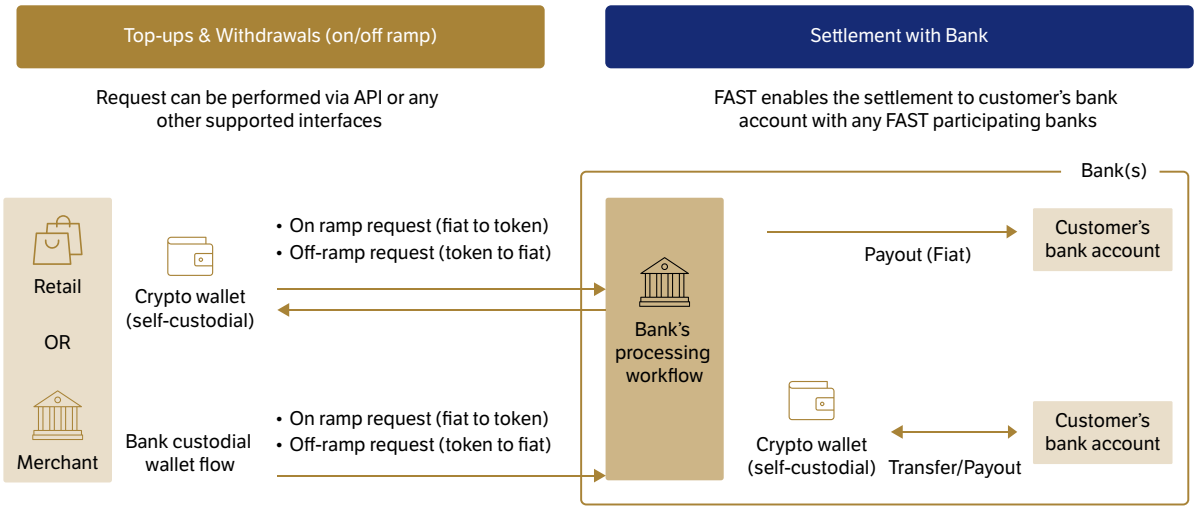


Figure 9: On-ramp and Off-ramp process

[15] Fiat money in this section of 5.3 PBM on-ramp & off-ramp specifically refers to notes, coins and bank deposits

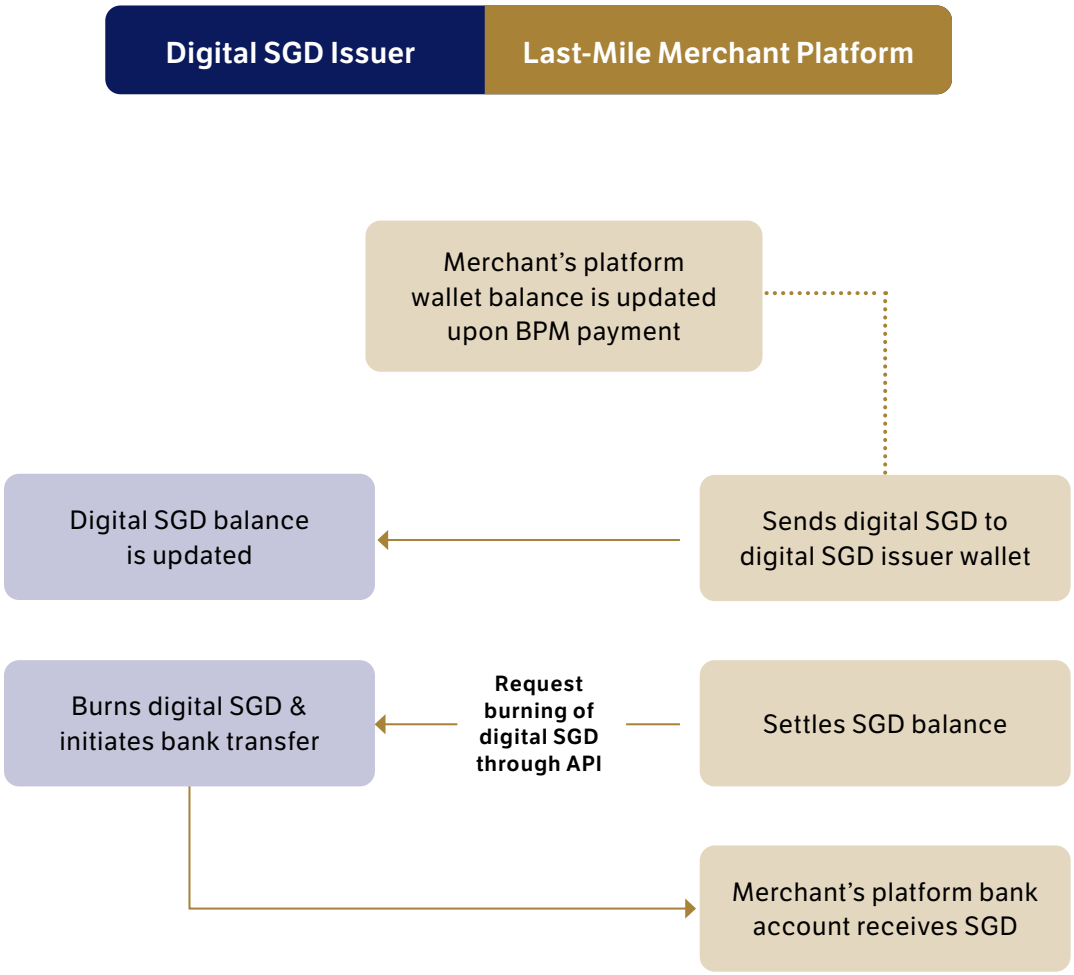


Figure 10: Digital SGD to SGD

5. PBMs will be made instantly available for users upon the completion of the airdrop. This also marks the end of the on-ramping process.

Off-ramp Experience

Meanwhile, for the off-ramp process, an emphasis is on the "last-mile" merchant acceptance of the underlying digital currencies.

1. Participating merchants need to be onboarded and equipped with a wallet to receive PBM payments. For example, Grab's wallet was used to facilitate payments and settlements for merchants for the commercial trial alongside the Singapore FinTech Festival 2022.
2. Designated merchant wallets are whitelisted by the PBM Creator and only transfers to these addresses will trigger unwrapping of the PBMs.
3. When a payment transaction is executed, the PBM is unwrapped automatically and the underlying digital currency token (i.e. digital SGD) is deposited into the corresponding merchant's receiving wallet.
4. For merchants to receive payouts in fiat into their bank account rather than digital SGD, the following steps would be required.
    - Once the digital SGD is sent to the merchant's wallet address, the digital SGD issuer receives API calls to burn digital SGD and initiate bank transfers of the equivalent amount of SGD to the merchant's corporate bank account.
    - For situations where customers have a crypto wallet with one bank, and CASA account with another. A FAST transfer between banks could be used to effect the settlement of traditional fiat pay-outs.

6 — Design Considerations

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

6.1 Interoperability

It is critical that introducing PBM and additional service providers do not lead to fragmentation in the payment ecosystem. If each PBM provider runs its own proprietary networks, it will lead to the creation of walled gardens with their own closed ecosystem of partners. This could lead to monopolistic, rent seeking behaviour amongst commercial firms. If left unchecked, this could be to the detriment of consumers, who will need to onboard to a myriad of different systems or pay exhorbitant 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. An approach to foster this is through the development of an open-sourced technical framework for PBM. To realise wide adoption, the governance behind the design and development of this technical specification, should be open with participation across different organisations. This will be key to ensure that the PBM technology acts in the interest of the public.

A standard data-exchange and API specification could be defined between wallet providers and PBM creators to achieve a standardized interface for PBM purpose parameters i.e. common merchant references such as UEN, SSIC etc to support whitelisting of retail merchants etc.

Future phases may involve studying integration with QR schemes – for example, there could be a mapping between the unique entity name (UEN) with a wallet address. By doing so, when a user scans the QR code, he or she would be able to select whether he or she wants to transact via current payment rails, or via this new payment rail. With that, PBM creators would not need to be concerned with merchant onboarding. As long as a merchant is onboarded to the common addressing scheme and has a wallet address, the PBM recipients would be able to make payments in their shop.

Another consideration is the integration and implementation of wallet providers that are closely associated with the national digital identity infrastructure. This opens the potential for easily crediting PBMs based on user identity and recipient requirements – such as means testing. This needs to be balanced with the need for user's personal data protection and privacy.

6.2 Fungibility of digital SGD across issuers

As long as there are multiple media of exchange by different issuers, some type of mechanism is generally required for them to be considered uniformly as currency, such that they can be used interchangeably for payments at their face value without being subjected to discounting or other frictions. Otherwise, differences across issuers, for example in the composition of their reserve backing, can lead to varying degrees of trust and confidence in their liabilities and hence the perceived value among end-users. This, in turn, prevents universal acceptance, which fragments liquidity and introduces significant inefficiencies into economic exchanges.

Today, central-bank issued money, bank deposits, and e-money are typically perceived to be "one and the same" regardless of their issuers. This fungibility between the different forms of SGD is secured through their guaranteed convertibility at par-value to central bank money (either physical cash or reserves). Notably, because MAS always recognises the monetary liabilities of different banks at their face value during the interbank settlement process, the exchange rate between all banks' deposits are effectively anchored at par. Regulation and supervision, together with the deposit insurance scheme, play a reinforcing role by helping to

establish a base level of trust in the liabilities of different issuers.

These mechanisms should likewise ensure that all digital SGD are fungible with each other and existing forms of money. Tokenisation in and of itself need not change the channel through which the value of privately-issued SGD is linked to central bank money.

First, MAS expects all future digital SGD issued in Singapore for use as a general medium of exchange to meet a minimum standard with regards to the surety of its value. This will be ensured through regulatory requirements (e.g., on the quality of the reserve backing, redemption at par, base capital and management of AML/CFT and cyber risks) on the issuer. For more information, please see MAS' consultation paper on the proposed stablecoin regulatory framework.

Second, participating intermediaries and digital SGD issuers can leverage on established payments and settlement infrastructure (e.g., Instant or Faster Payment Systems and Real Time Gross Settlement Systems (RTGS)) to settle off-chain the outstanding obligations that arise when they end up holding tokens from other issuers. Banks will play a vital bridging role in this case, given their access to MAS' balance sheet—the convertibility of digital SGD to central bank money is achieved first through its conversion into bank liabilities via the off-ramp processes, which generates outstanding interbank liabilities that is subsequently settled through MEPS+ (Singapore's RTGS).

CBDCs may offer new bridging possibilities that ensure the fungibility between different forms of digital SGD. A wholesale CBDC platform could serve as a more advance iteration of a common settlement infrastructure such as MEPS+ that allows for new capabilities such as atomic settlement between participating financial institutions. The platform could potentially be an avenue through which a wider range of financial institutions, including stablecoin issuers, can gain access to central bank liabilities for settlement purposes. A retail CBDC goes even further as holders of digital SGD would not need to go-off chain to access central bank money.

6.3 User Protection

The nascency of PBM technology and digital currency, means that without prior knowledge, users might find it difficult to differentiate between a genuine PBM token and digital SGD, and attempts to defraud them. For example, although PBM token smart contract addresses are unique; token names do not necessarily have to be unique. Therefore, it is possible for a third party to create another token with the same token name and advertised as such even though it has a completely different smart contract address. Malicious actors could take advantage of this by scamming the public into transacting with the fake token instead. This risk is elevated if public and permissionless blockchains are used.

However, it is unlikely for two different tokens with the same exact name to be in public circulation as no centralised or decentralised exchange would list two tokens with the same exact name. Furthermore, consumers and merchants can check the smart contract addresses of tokens which are publicly available and can be identified through the creator's digital wallet address or using the list of historical transactions available from the blockchain. Nevertheless, before any full-scale public rollout, it is envisioned that broad based public education is needed to assist the public to mitigate against the risk of scams.

To prevent unintended speculation and abuse, the secondary trading of PBMs can be restricted through controls programmed within the smart contract. For example, the moment a PBM is used for payments, the underlying value will be unlocked and the PBM will be destroyed. Additional controls can be built into the smart contract such that transfers of PBM can only be done once, restricting further transfers.

6.4 Operational Cost

A motivation for implementing a PBM based infrastructure is that the overall transaction cost should be low, or minimally lower than the cost of existing systems.

For example, if PBM is implemented on public blockchain based infrastructure, fees are payable to validators in the network and this increases as more people demand for transactions to be processed in the ledger. One mitigant would be to transfer the actual cost of the transactions from the PBM holder to the PBM Creator via a gas station network, where the real gas fees is paid by the PBM Creator and the PBM holder is charged a smaller fee determined by the PBM Creator. Such an arrangement will be similar to existing approaches, whereby payment service providers can choose to absorb the transaction cost or pass it on to consumers.

Beyond immediate transaction fees, there would be additional costs of building, operationalising, onboarding merchants and parties to digital SGD and PBM technology. Any such system would then need to ensure that the overall cost of the system is kept low for it to be a viable alternative.

6.5 Digital Readiness

Electronic payments and the adoption of digital technology in Singapore has accelerated in recent years. However, the introduction of any new forms of payment instrument in the form of a digital SGD would likely require some adjustment to the user experience and might be viewed as disruptive by some.

The digital savviness of the stakeholders is applicable to the design of the PBM scheme as well. For government disbursement, this refers to merchants as well as the voucher recipients. 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 digital SGD and PBM.

Given this, further design considerations would have to be in place to determine if digital SGD is a viable alternative to traditional cash. It is important that special care be made to keep the user experience intuitive and accessible especially to more vulnerable segments of the population.

Future research may include studying options for offline payment for low-value payments to reduce network reliance and support financial inclusion within the country.

6.6 Security

If users lose their private keys to their digital wallets, there is no feasible way to get back access to the contents of their digital wallets. This also means that any digital asset or PBM that is stored within that digital wallet will be inaccessible to any party. One way to mitigate this risk is the creation of a credentials management module by an accountable party to preserve the private keys of digital wallets on behalf of users. Therefore, if users lose their private keys, they would be able to retrieve their keys via a login ID and password from the party. Another approach is to invalidate the underlying backing digital currency and reuse an equivalent amount to the user. This will, however, require coordination with the issuer of the underlying digital currency.

Smart contracts, which are self-executing code that contains the business logic for digital currency-based solutions, might be targeted by malicious actors who seek to exploit vulnerabilities in the smart contract code to drain funds or to manipulate the market, leading to a loss of confidence. Aside from reviewing the code itself, a thorough review of the information security process would need to include the full development and deployment lifecycle as well.

Aside from guarding against the initial exploit, incident management is important as well.

Unlike centralised systems with a known operator, blockchain based networks, relies on consensus from a group of participating validating nodes (which are sometimes anonymous) to preserve the integrity of records. Consequently, in the event of an exploit, it would be much harder to organise a coordinated response such as blocking a transaction.

Given the experimental nature of the initial phase of Project Orchid, the trials conducted by industry participants involved a restricted group of trial participants and merchants, with low value and limited number of transactions. Hence, a thorough security review and recommendation is not in scope. This will need to be revised in subsequent phases of Project Orchid.

6.7 Anti-Money Laundering and Countering Financing of Terrorism

While a seamless user experience is an important design goal, it is equally paramount to ensure that there is a proper procedure to conduct risk assessment and enforce anti-money laundering (AML) and countering the financing of terrorism (CFT) commitments.

PBMs are designed to be used in a permissioned ecosystem and for payments of goods and services that are provided by approved merchants. This is to mitigate money laundering and terrorist financing risk concerns. As PBM is extended to other use cases in future, additional safeguards and risk appropriate measures may need to be introduced. To mitigate risks, the digital SGD issuer, the merchant wallet provider and the entity handling the last mile settlement would need to be a regulated bank or payment institution.

- The digital SGD issuer mints and provisions the underlying digital currency backing the PBM in accordance to the terms and conditions prescribed by the PBM Creator. The PBM

Creator will receive the PBM from the regulated financial institution who wraps the digital SGD and delivers the PBM to the PBM Creator.

- The PBM Creator will need to have an account with the digital SGD issuer and the digital SGD issuer will perform AML and CFT controls, including client due diligence (CDD), on the PBM Creator.
- As part of the onboarding process, AML/CFT controls, including CDD, will be conducted on the merchants and PBM holders. For example, DBS and Grab will conduct CDD on the merchants given that they are providing banking/wallet services to these merchants and processing the last mile settlement.
- If the PBM holders are using a crypto wallet provided by a regulated VASP, the expectation is that the regulated virtual asset service provider (VASP) would conduct CDD on the PBM holder.

An unresolved risk is that PBM holders may use un-hosted wallets, for example for peer-to-peer transfers. This may mean that users of PBM may not be subject to KYC checks. It is not clear to us that AML/CFT risks can be fully mitigated in such cases.

An intermediate approach could be to limit the amount that can be transferred between anonymous wallets. Consequently, from a consumer perspective, value transfers could be entirely anonymous, only requiring more information when the transaction value crosses above a certain threshold.

Alternative approaches include the use of verifiable credentials as a mechanism to determine if the PBM holder is a verified user.

Aside from the initial onboarding, ongoing due diligence, and transaction monitoring, such as setting alerts and parameters, are deemed industry best practices and required for financial institutions.

As PBM is extended to other use cases in future, additional safeguards and risk appropriate measures may need to be introduced.


DBS
HSBC
OUE


Maybank
FWD

7 — Case Studies

7.1 Case Study 1 – Government Vouchers

Background

RedeemSG is a government voucher system developed by OGP, GovTech to make it easier for government agencies to start and manage a voucher campaign. RedeemSG is used today by agencies such as NEA, the Public Utilities Board (PUB) and People's Association (PA) for the CDC voucher scheme.

The experience working with campaign organisers has informed the RedeemSG team about the common challenges faced by both the public and private sector when organising government disbursements. These challenges as highlighted in 4.1 Government to Person, include the high cost of implementing voucher schemes and the speed of settlement and reconciliation.

Based on feedback from more than 20 Government agencies, the following core requirements for government voucher campaigns were identified:

- Government vouchers are organised in terms of specific schemes, or in RedeemSG terms "Voucher Campaigns" run by "Campaign Organisers"
- Typically, requirements should apply consistently throughout a 'voucher campaign' to ensure each recipient receives the same amount (e.g. within the same scheme, a recipient always gets $50)
- Vouchers can be created for monies earmarked by the Government Campaign Organiser, where the Sum of Total Vouchers is less than or equal to the monies set aside
- Vouchers can be redeemed at specified merchants - this is required especially in the public good context, where Government provides funds towards a certain public good objective (e.g. vouchers to promote healthy living should be spent only at participating merchants with healthy food)
- Merchants should be reimbursed quickly, once the voucher is redeemed.
- The amount for which the merchant is reimbursed should be equal to the value of each voucher transaction
- The voucher will expire on the prescribed expiry date

As part of ongoing efforts to improve RedeemSG, OGP aims to embed the verification checks on the authenticity of vouchers directly into the digital voucher issued to citizens. In addition, it is desirable that merchants receive their payout immediately when a voucher is used as it will improve their cashflow. The implementation of a common ledger that is immutable, time and date-stamped and is transparent to all parties involved, will reduce reconciliation efforts. Finally, the design should be flexible to cater for the most complex of voucher requirements.

Approach

OGP partnered with DBS Bank to test the use of PBM to support government disbursement. The initial pilot involves the issuance of PBMs to select retail individuals. For the purpose of the pilot, DBS Bank issued digital SGD in the form of tokenised deposits.

Role	Party
Digital SGD Issuer	DBS
Last Mile Settlement	DBS
Merchant Wallet Provider	DBS
PBM Creator	OGP
PBM Holder	Select Retail Individuals
PBM Redeemer	Merchants

Table 3: Parties involved in the Government Vouchers pilot

Through this pilot, OGP aims to achieve the following goals:

1. **Demonstrate faster payouts to merchants**
   The trial tests the concept of having merchants directly receive the underlying digital SGD for the vouchers redeemed. In the longer term, when digital SGD is widely accepted, merchants would be able to use digital SGD immediately to pay for their next set of transactions. However, as digital SGD issued by DBS Bank is not recognised to be legal tender and widely circulated at this time, digital SGD is converted to deposits in the merchant bank account at the end of day.
2. **Demonstrate feasibility of adopting smart contracts for Government campaigns**
   Government campaign organisers should be able to easily define and enforce their voucher logic (e.g. targeted merchants, specific timeframe) and issue vouchers to their targeted users. If vouchers are used outside of the terms of the smart contract (e.g. at merchants not participating in the scheme), the transaction should fail.
3. **Demonstrate interoperability across voucher schemes**
   Campaign organisers should also be able to easily specify their own required voucher logic, without the need to re-invent existing voucher systems. In the long term, recipients should have the freedom to choose their own wallet applications to access Government issued PBM tokens.

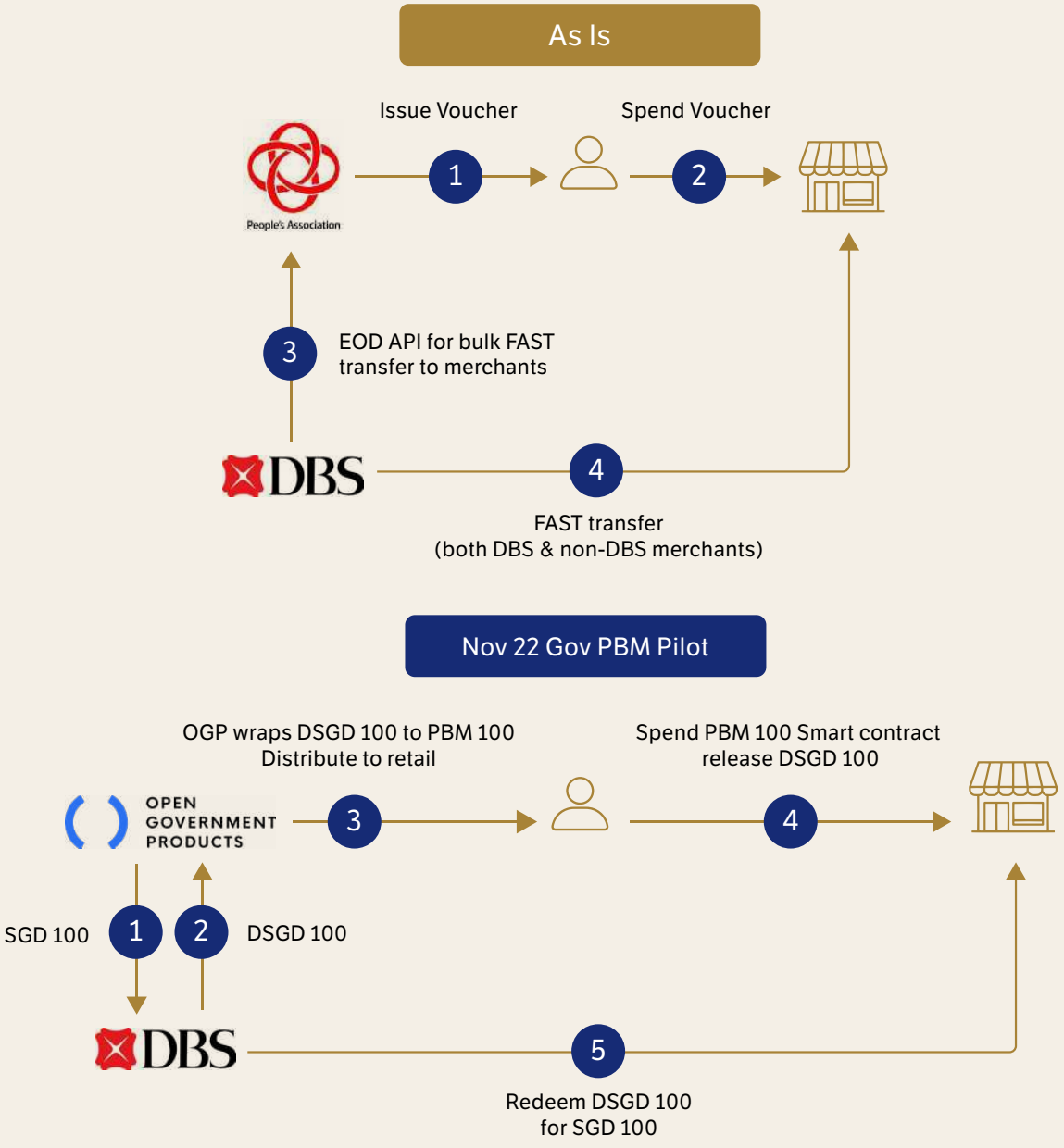


Figure 11: Comparison of current CDC Voucher flow versus Pilot

The government voucher trial consists of the following steps:

1. PBM Creator deposits funds that is intended to be used for this trial with the digital SGD issuer
2. Digital SGD Issuer proceeds to mint the digital SGD based on the funds sent by the PBM Creator.
3. PBM Holder onboards and receives voucher: The voucher recipient first sign up for the campaign with the PBM Creator. For this trial, the PBM Creator will then create an ephemeral Crypto Wallet for the holder and map this wallet to an existing identifier. The voucher (PBM) holder will then be sent a unique voucher link via SMS, containing their wallet information. During payment, the PBM holder, goes through the process of selecting the amount, the merchant before confirming payment. Once successful, the PBM holder will show the success message to the merchant.

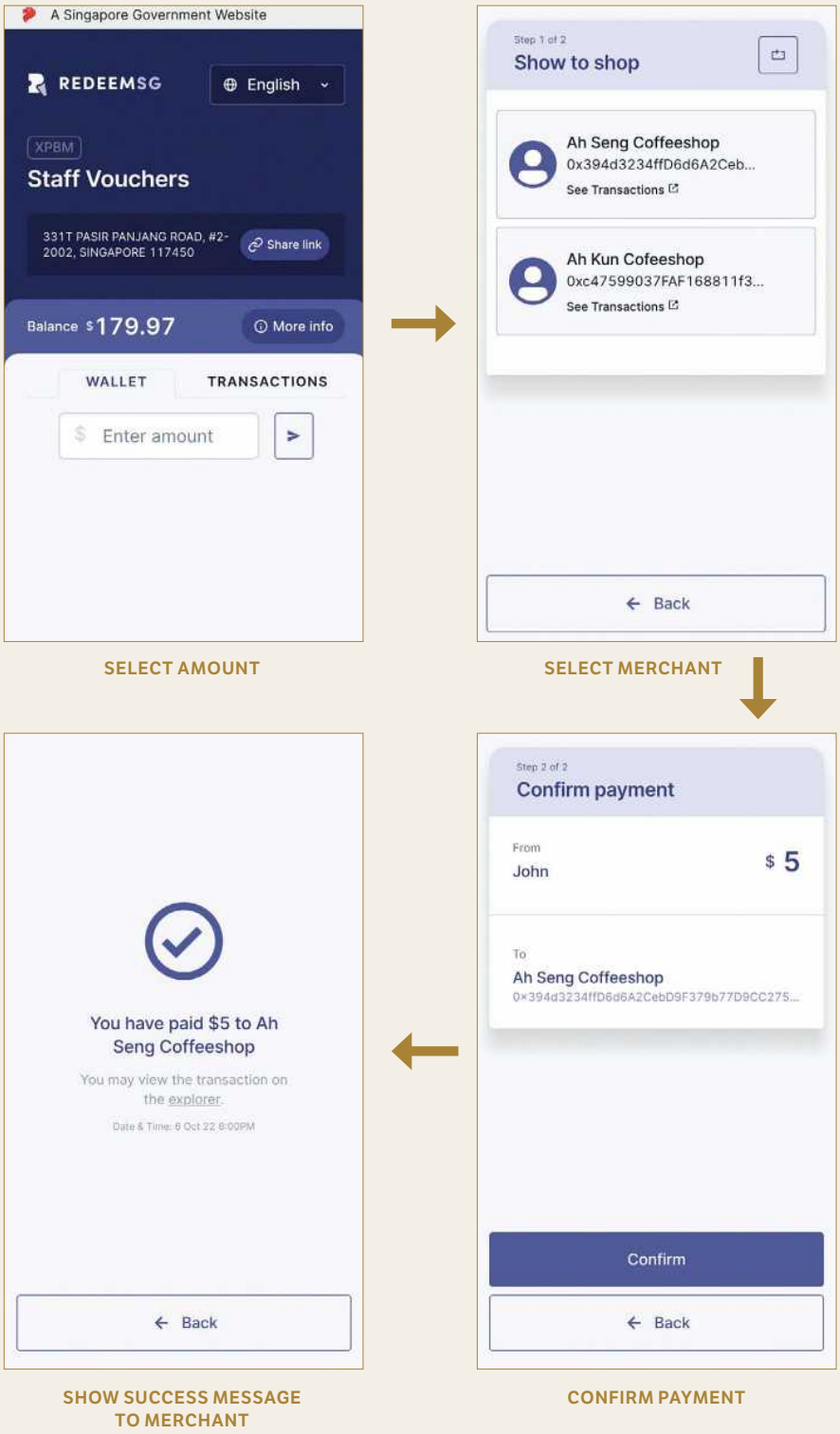


Figure 12: PBM Holder/Voucher Recipient's view

Upon creation, the wallet address will be returned to OGP and these addresses will be added to the “approved” merchant list within the PBM contract.

4. **PBM Redeemer (Merchant) Onboarding:**
   Merchants will first sign up with OGP. OGP then proceeds to send the merchant’s bank account number to DBS for the creation of their wallet. Upon creation, the wallet address will be returned to OGP and these addresses will be added to the “approved” merchant list within the PBM contract. OGP will send a unique link to the merchant via SMS that the merchant can access to see transactions and payouts. As soon as payment is initiated, the PBM contract will validate whether the merchant address is in the “approved” list and approve or reject the unwrapping of PBM to Digital SGD accordingly. If successful, the merchant receives a notification about the transaction. The merchant may also view history of transactions via the provided application.
5. **Pay-outs**
   At the end of each day, DBS Bank will transfer all Digital SGD from the merchant’s wallet back to the bank’s wallet. After which, DBS will proceed to burn the Digital SGD, release the earmarked SGD and transfer it to the Merchant’s Bank Account.

Additional Considerations

In this new approach, OGP decided to use a user-initiated user flow for transactions, in place of the current RedeemSG interface which is merchant-initiated. This was to design for possible integrations with SGQR in the future.

In addition, for purposes of this limited trial, the target users were assumed to be digitally savvy and paper vouchers would not need to be catered for. Hence, unlike the existing RedeemSG system, there was no longer a need to issue vouchers in specific denominations.

Another core design decision made was to keep the user experience simple for merchants. Participating merchants need not have any knowledge of PBM tokens, instead they receive only Digital SGD. This approach is similar to that of RedeemSG, where merchants are only concerned with payouts to their bank accounts, rather than the underlying mechanics of the voucher scheme they are part of.

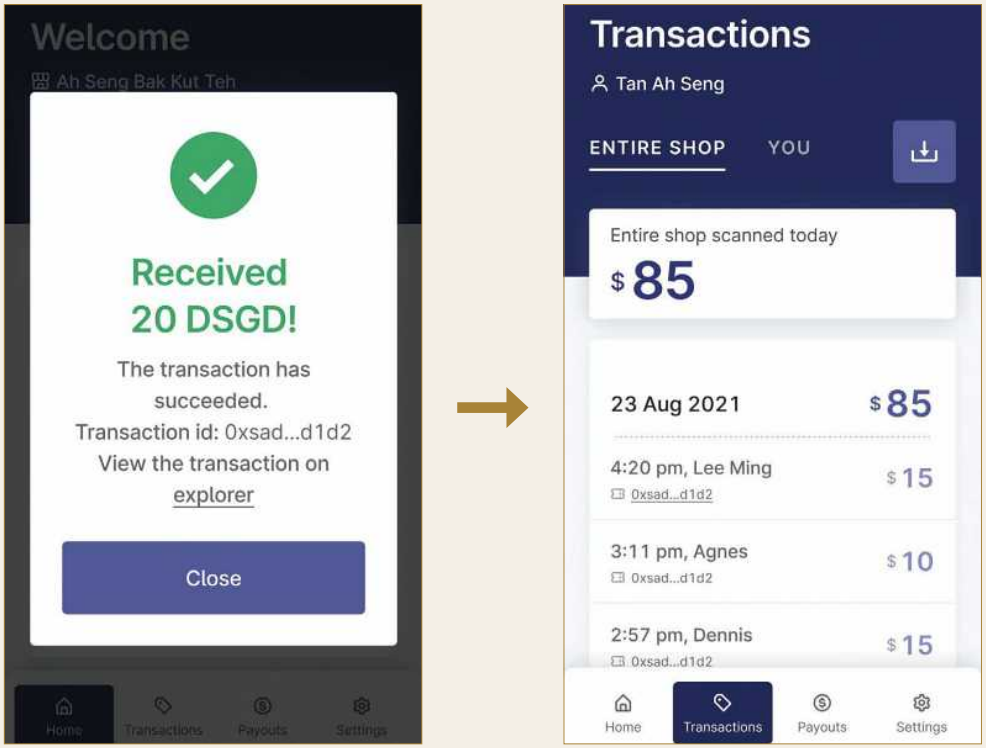


Figure 13: PBM Redeemer/Merchant’s view

7.2 Case Study 2 – Commercial Vouchers

Background

Existing voucher schemes tend to be manual, and paper based. While efforts are underway to digitise vouchers and consolidate rewards programmes, the customer experience remains fragmented. Consumers do not have a choice on the channel to view or use these vouchers, as access is typically through proprietary applications, provided by individual voucher issuers or campaign organisers. To compound issues, users and merchants could be inundated at a given time with different vouchers, having to read and understand the terms and conditions for each scheme. In this context, PBM holds the potential to address the gaps in existing commercial voucher schemes.

Approach

Alongside the SFF 2022, trials of PBM based commercial vouchers were conducted by industry participants led by Temasek, Fazz and Grab. Participants experienced using different PBMs to make payments to different vendors for different purposes within and outside of the main SFF venue. Participating trials included:

- PBMs in the form of SFF vouchers were distributed to trial participants to offset purchases at participating food and beverage merchants at the main SFF venue at the Singapore Expo.
- Participating merchants from Grab's ecosystem supported the use of PBM where SFF side events were held.

Role	Party
Digital SGD Issuer	Fazz
Last Mile Settlement	Grab
Merchant Wallet Provider	Grab
PBM Creator	Corporate Partners
PBM Holder	Selected SFF Participants
PBM Redeemer	Merchants

Table 4: Parties involved in Commercial Voucher Pilot

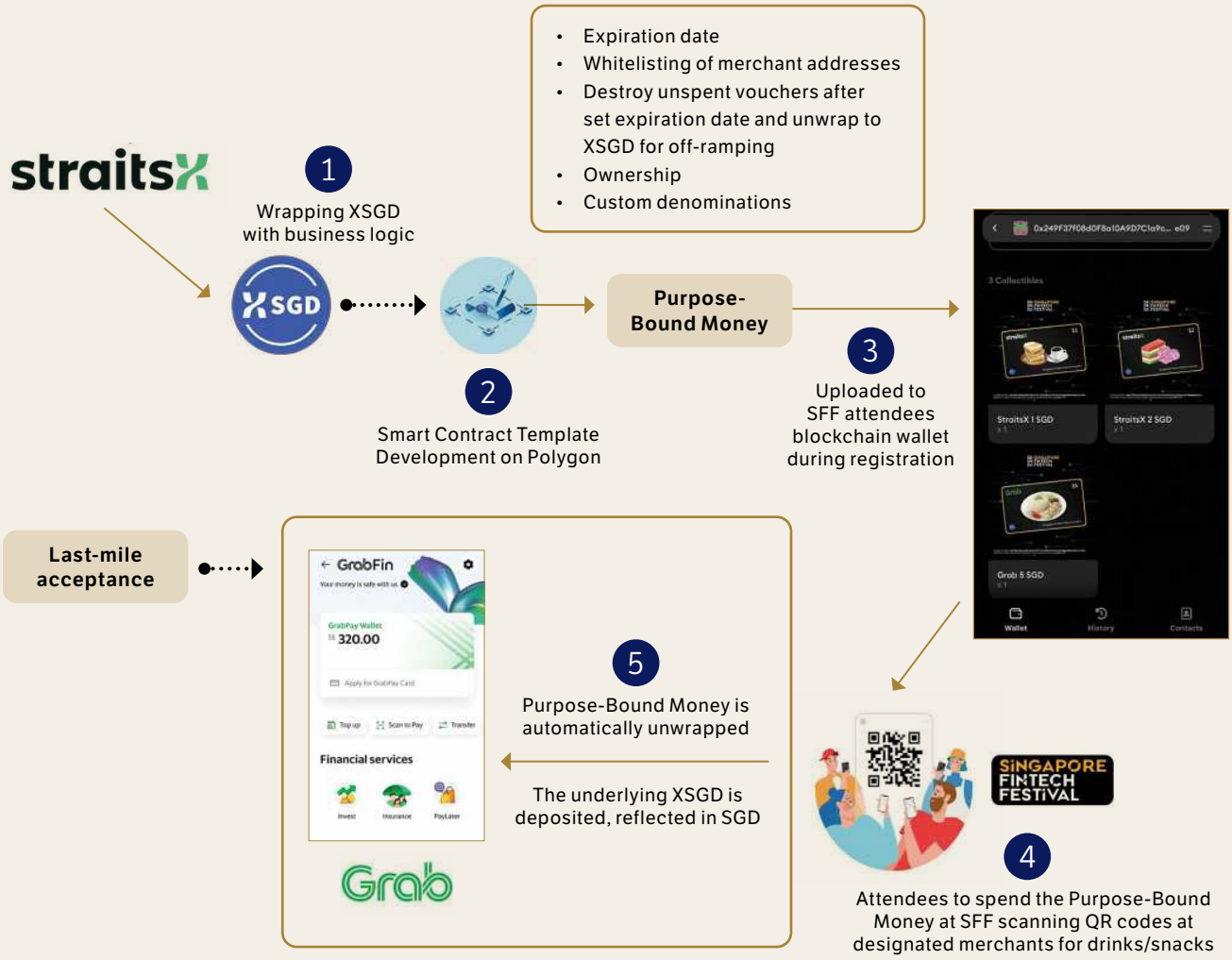


Figure 14: Overview of Commercial Voucher Pilot

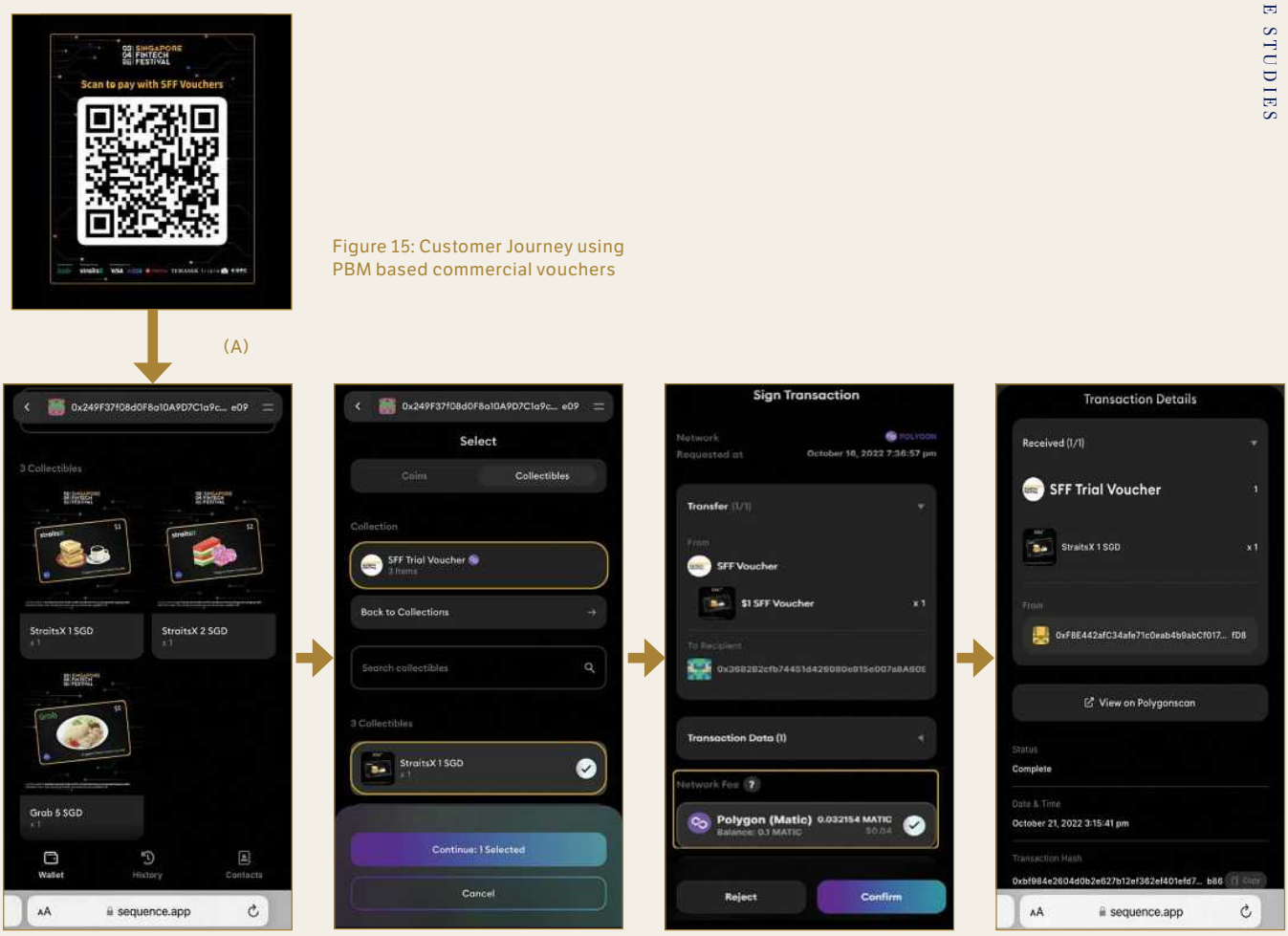


Figure 15: Customer Journey using PBM based commercial vouchers

Overall, there are five major steps involved in the trials.

1. First, XSGD, the SGD pegged stablecoin, is minted to be used as the underlying medium of exchange.
2. Secondly, the conditions for use are programmed at the smart contract level. The "wrapped" token created is the PBM. It is important to note that the PBM is built on top of the ERC-1155 contract standard due to its semi-fungibility. The design choice of ERC-1155 is intentional to maximize flexibility to accommodate different types of PBM structures within the same contract.
3. To distribute the complimentary PBMs to attendees, the PBMs were airdropped to trial participant's wallet addresses. To ensure transaction security and prevent illicit on-chain activities, StraitsX (part of Fazz) leveraged a predictive digital assets risk and intelligence platform to screen the blockchain wallet addresses submitted by participants. The PBM is interoperable with both custodial and non-custodial wallets that support ERC-1155 standards.
   a. Once attendees receive the PBMs, they can view the PBMs in their individual wallets.
   b. Attendees can open the wallet to scan the QR code.
   c. The attendee selects the PBM to be used.
   d. Attendees review the wallet address, selected PBM, network fee. Attendees confirm the transaction.
   e. PBM is successfully sent and accepted into the merchant's Grab wallet where it will be automatically unwrapped into XSGD and reflected in SGD.
4. Merchants, as part of this pilot use Grab wallets to receive PBM payments. Designated merchants' wallets have been whitelisted in advance. Only when a PBM is sent to a whitelisted address will the PBM be unwrapped and the underlying XSGD be deposited into a merchant's Grab wallet. Grab leverages TripleA and StraitsX's capabilities as Digital Payment Token (DPT) payment processors to accept XSGD and off-ramp to SGD.

5. The merchant balance is reflected in SGD, marking completion of the settlement as well as the "last-mile" acceptance of the PBM. From a merchant's perspective (step 5), they will receive a notification that the PBM has been received and this will be reflected in their Grab wallet as SGD:

Additional Considerations

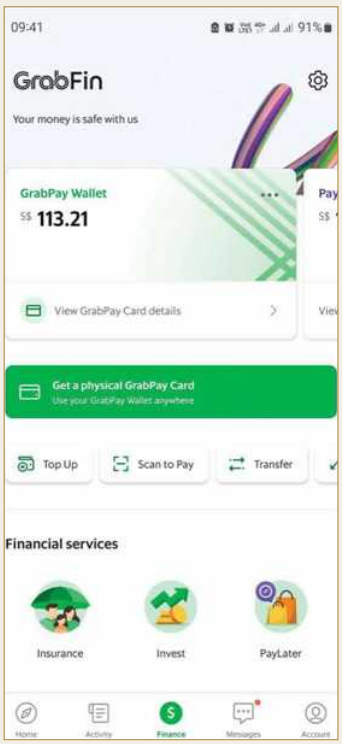


Figure 16: Merchant receives notification on PBM acceptance

After the trial period, unused or expired PBM vouchers will lapse, and the underlying XSGD will be retrieved and returned to the PBM Creators. The image of the voucher, however, will remain in a user's wallet as an ERC-1155 token. Programmed in the smart contract, the image will be updated to indicate that the voucher is no longer valid as a payment method.

As an additional safeguard, a control feature is introduced into the smart contract that can pause transactions. This offers the PBM Creator the option to stop all interactions with the NFTs to mitigate speculative risks and exercise control to prevent peer-to-peer transfers and potential secondary trades of the tokens.

7.3 Case Study 3 – Government Pay-outs

Background

OCBC Bank supported the Central Provident Fund Board (CPFB) in launching the GovCash cheque replacement service in 2021. The service enables Singaporeans who are unable to use direct bank crediting to receive government payments via facial recognition at OCBC's ATMs without needing to have an OCBC bank account. In addition, as part of GovCash, OCBC has collaborated with GovTech on the LifeSG app, which enables Singaporeans and Singapore Permanent Residents to view government payments deposited into GovCash via the LifeSG app. Through the service, users can transfer payments into their PayNow-linked bank accounts and pay merchants by scanning the QR codes.

Building upon the work started with GovCash, OCBC Bank and CPFB aim to take the national digital payment services to new heights by designing and testing a solution that uses the digital SGD and PBM smart contract, reducing overheads of the fund disbursement process from CPFB to the intended recipients.

Approach

Starting with a proof of concept, OCBC Bank and CPFB will test the technical viability and programmability of the digital SGD and PBM Solution to seamlessly and efficiently support end to end disbursement of funds to the intended recipients through a controlled environment.

- A test disbursement scheme will be setup with end-to-end process for disbursement of funds on existing FIAT payment rails
- Disbursement will be done to a small group of CPFB recipients who are OCBC customers
- The test will be conducted on the OCBC Enterprise Blockchain Platform, a permissioned Ethereum Virtual Machine based platform.

Role	Party
Digital SGD Issuer	OCBC Bank
Last Mile Settlement	OCBC Bank
PBM Creator	OCBC Bank
PBM Holder	A select group of CPFB recipients

At this stage, the digital SGD and PBM smart contract framework are transparent to the recipients as the solution will only be used to facilitate fiat payments to the designated recipients. Digital SGD and PBM will not be directly accessible or usable by the public and remain within the OCBC's permissioned enterprise blockchain.

Recipients will only be able to receive the disbursment from CPFB through the existing FIAT payment rails, such as funds transfer to PayNow NRIC-linked bank accounts or cash.

The PBM smart contract solution will be designed and built to be scalable and interoperable with external networks to support extended use cases and will be the underlying foundation for OCBC Bank to integrate with a regulated digital currency settlement rail. The introduction of digital currency-based settlement rails will help to overcome limitations and other inefficiencies that exist in current FIAT rails.

The PBM smart contract solution will be designed and built to be scalable and interoperable with external networks to support extended use cases and will be the underlying foundation for OCBC Bank to integrate with a regulated digital currency settlement rail. The introduction of digital currency-based settlement rails will help to overcome limitations and other inefficiencies that exist in current FIAT rails, e.g., FAST maximum limit of SGD200,000 per transaction.

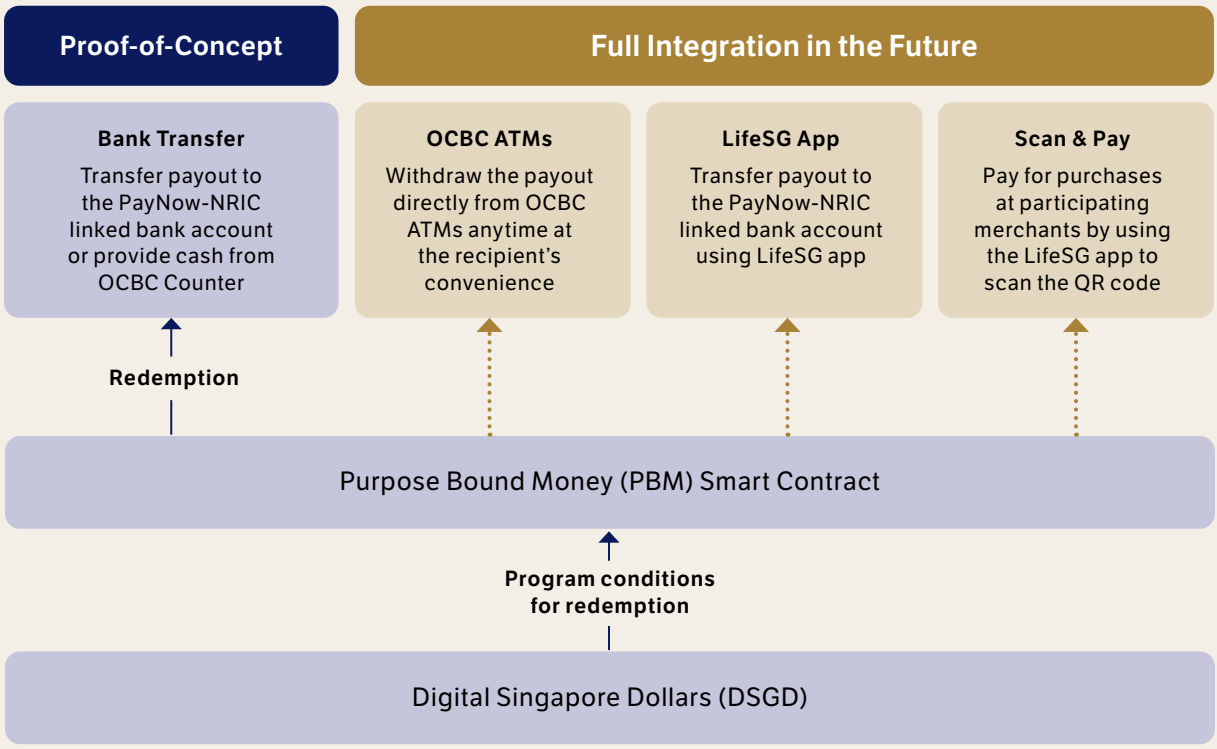


Figure 17: Overview of Government Pay-out Pilot

7.4 Case Study 4 – Learning Account

Background

Governments provide various types of fiscal transfers to citizens with the intention of supporting a target citizen segment or stimulating the local economy. In working through grant schemes, the public sector will need to address challenges such as the cost of implementing grant schemes, long settlement processing time, and fraudulent claims and exploitation of government pay-outs.

Grant schemes could be in the form of supporting learning and skills mastery of the population. These would involve the provision of learning accounts to eligible citizens and businesses and include training institutions, who need to be pre-approved by government agencies.

For example, SkillsFuture Singapore (SSG) may provide fiscal transfers to citizens and businesses in a controlled, efficient, and secure manner.

Approach

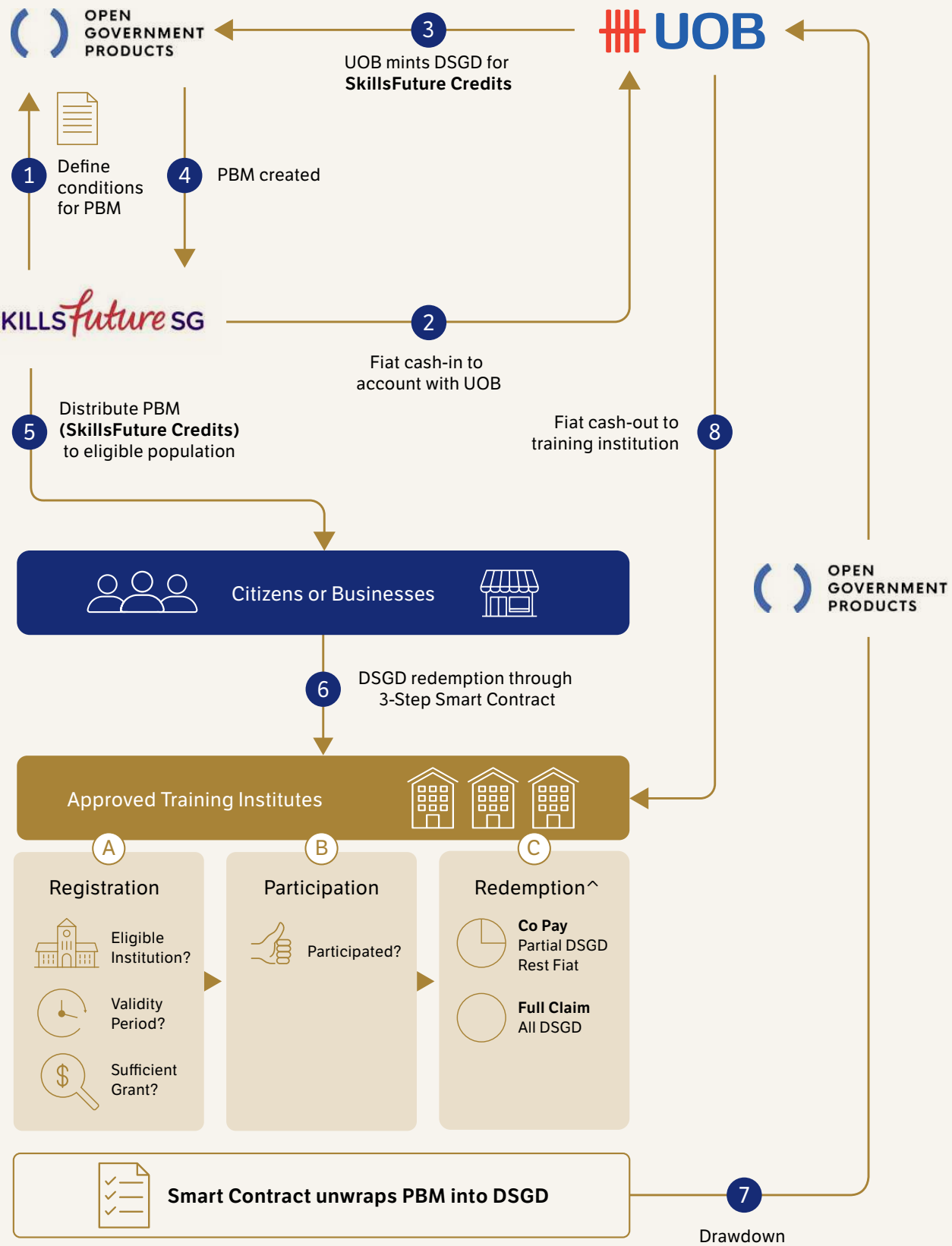
UOB will partner with OGP to pilot this initiative:

- UOB will be responsible for implementing Digital SGD Smart Contract.
- OGP will be responsible for implementing PBM that will wrap and unwrap Digital SGD using ERC-20 standards.
- UOB will be responsible for providing Wallets to Approved Training Institutions.
- On-ramp and off-ramp activities will be transparent to Approved Training Institutions and be handled by UOB.

The trials will involve the following steps:

1. The PBM Creator, will define the conditions for using the learning account. This is translated to a smart contract code.
2. The PBM Creator transfers funds into their UOB account.
3. UOB as the digital SGD issuer will mint the Digital SGD that will be utilised towards the learning account.
4. The PBM supporting the learning account is now created.
5. The learning account in the form of a PBM is distributed to eligible citizens or businesses.
6. Next, the redemption of the underlying digital SGD occurs through a 3-step verification process implemented as a smart contract, which checks the following:
    a. **Registration –** eligible participants' enrollment on approved training providers before grant expiry.
    b. **Participation –** Training Institutions indicate that the individual participated in the learning.
    c. **Redemption –** If above conditions are met, grants are released from the citizen wallet to the Training Institutions.
7. Once the conditions are met, the PBM is unwrapped, and the training institutions receives digital SGD.
8. As a final step, the training institutions could convert their digital SGD into funds in their deposit accounts with UOB.

Role	Party
Digital SGD Issuer	UOB
On-ramp and Off-ramp responsibility	UOB
Merchant Wallet Provider	UOB
PBM Creator	SkillsFuture Singapore
PBM Holder	Citizens or Businesses
PBM Redeemer	Approved Training Institutions



^Supports both partial and full payment terms
- Partial – partial **SkillsFutureCredits** (DSGD); remainder Fiat (Cash)
- Full – where DSGD is sufficient

Figure 18: Overview of Learning Account Pilot

8 — Summary and Next Steps

The first phase of Project Orchid brought together different stakeholders in Singapore through a common initiative to understand the potential opportunities and drawbacks of introducing a programmable digital SGD. The project also introduced a new concept, the idea of PBM and its application in Singapore.

The project sought to achieve the right balance between tapping the possibility of emerging technologies while ensuring that the initiative remains pragmatic and grounded in addressing today's problems and context. The diversity of the industry group, from the public and private sector, added to the richness of the learnings from the project.

Through the contributions of the industry group, an initial set of use cases for digital SGD has been identified. To better understand the user journey and gather feedback, trial events were conducted to refine product features and optimise the user experience. Some of the use cases will be tested through live trials by the public and the private sector in 2022, and others will be conducted in 2023. The ongoing pilots are expected to yield valuable insights and advanced the learning even further.

In subsequent phases, Project Orchid will engage with a broader set of stakeholders and investigate a greater set of capabilities. Future research areas include the integration of a common QR code system, the fungibility of digital currencies amongst different issuers, transactional privacy, offline payments, digital wallet integration, and future trials where individuals could have options to define conditions for transfers and be PBM Creators in effect.

Developments in digital currency are rapidly evolving, consequently there may be further enhancements and innovations that might not have been identified. Nevertheless, MAS envisions that the efforts from the initial phase of Project Orchid would serve as the foundation for developing a financial infrastructure capable of meeting the current and future needs of corporates, merchants, financial institutions, FinTechs and the public at large.

9 — Acknowledgements

Steering Group			
Name	**Organisation**	**Name**	**Organisation**
Alan Lim	Monetary Authority of Singapore	David Woo	NETS
Emilia Lee	Monetary Authority of Singapore	Lena Tan	NETS
Shee Tse Koon	DBS Bank	Melvyn Low	OCBC Bank
Ng Peng Khim	DBS Bank	Peter Koh	OCBC Bank
Tianwei Liu	Fazz	Laura Loh	Temasek
Aymeric Salley	Fazz	Kevin Lim	Temasek
Wong Wenbin	Grab	Janet Young	United Overseas Bank
Nikhil Dwarakanath	Grab	So Lay Hua	United Overseas Bank

Contributors			
Name	**Organisation**	**Name**	**Organisation**
Vincent Pek	Monetary Authority of Singapore	Roy Wong	NETS
Ling Yan Toh	Monetary Authority of Singapore	Kwan Hoon Park	OCBC
Edison Leo	Monetary Authority of Singapore	Ravindra Kumar	OCBC
Low Ze Sheng	Monetary Authority of Singapore	Janice Lee	OCBC
Raihan Zulimran	Monetary Authority of Singapore	Jorden Seet	OCBC
Elicia Chuah	Monetary Authority of Singapore	Adeline Ng	OCBC
Tay Zhenqian	DBS Bank	Talitha Chin Rui Ling	Open Government Products
Alan Hwong Wen Shuen	DBS Bank	Tay Paul Hong	Open Government Products
Chua Wang An	DBS Bank	Sheikh Salim Bin Mohamed Aneess	Open Government Products
Li Zilong	DBS Bank	Pallanikumaran	Open Government Products
Raymond Chong Tze Wei	DBS Bank	Jeannie Lim	Grab
Mihir Mohan	Fazz	Marianne Tee	Grab
Gloria He	Fazz	Michelle Chou	Grab
Victor Tan	Fazz	Zhu Qiuxuan	Grab
Adimas Prasetiyo	Fazz	Ho Giao Pik	United Overseas Bank
Terence Teo	Fazz	Hoong Chi Ming	United Overseas Bank
Stephen Lee	NETS	Varun Rally	United Overseas Bank
Desmond Goh	NETS	Lyselle Tan	United Overseas Bank
Jocelyn Ang	NETS	Ng How Xiang	United Overseas Bank
Ang Sok Hong	NETS		

Additional contributions from MAS departments

- Economic Policy Group (EPG)
- Anti-Money Laundering Department (AMLD)
- Payments Department (PD)
- Prudential Policy Department (PPD)

Additional contributions from other organisations:

- CPF
- Garçon Design
- SkillsFuture Singapore

Annex 1: Central Bank Digital Currency

A CBDC is a digital payment instrument, denominated in the national unit of account, that is the direct liability of the central bank (BIS et al., 2020). CBDCs can be further distinguished between wholesale or retail use. A retail CBDC is one that is meant for use by members of the public for payments. It would be the digital equivalent of the notes and coins that central banks issue today. A wholesale CBDC, in contrast, is one whose use is restricted to a select group of financial institutions, primarily made up of commercial banks. It is the equivalent of the reserves commercial banks place with the central bank today.

As with any form of money in existence today, there are two main elements to a CBDC, namely the monetary object itself (i.e. the financial liability or value), and the infrastructure that enables the transfer of this value. This infrastructure includes everything from the database on which CBDC is recorded, to the applications and point of sale devices that are used to initiate payments (BOE, 2020).

The defining characteristic of a CBDC is its direct claim on the central bank. This suggests that a key policy consideration is access to the central bank's balance sheet: Who should have access and in what form? How important is it to have direct access to central bank liability? Today, everyone has access to a liability of central banks, albeit only in the form physical banknotes and coins. In comparison, only a select group of financial institutions (primarily banks) currently have access to a digital form of central banks' liabilities, i.e. reserves.

There have been proposals for "synthetic CBDCs"—digital currencies issued and managed by private payment providers that are backed one-for-one by central bank reserves. These are considered a special form of stablecoins, which are likely to be uniquely safe among stablecoins given its central bank reserves backing. Nevertheless, as liabilities of private sector firms, "synthetic CBDCs" will arguably not have the same degree of riskless-ness or liquidity as central bank-issued CBDCs. Conversely, they could preserve a comparatively larger role for the private sector, and hence the benefits of private sector innovation, than might be envisioned by some retail CBDC arrangements.

Annex 2: Tokenised Deposits

An emerging area explored by commercial banks is the concept of tokenised bank liabilities.Tokenised deposits, issued by regulated and licensed commercial banks, are the digital representation of existing liabilities of the bank, with claims held by the token bearers. They are designed differently from stablecoins (refer to Annex 3 for more information).

Banks are exploring the use of tokenised deposits, based on DLT, to enhance their payment and settlement capabilities while aiming to have minimal impact to the banks' risk exposure, business model and regulatory obligations. It is important to note that this does not mean that the traditional deposit accounts will be decentralised and placed on the blockchain or that the tokenised deposits are necessarily accorded the same depositor protections as regular bank deposits. Rather, the goal is the additional creation of programmable money that could be used within the framework of smart contracts, which in turn permits for more efficient transactions and refined payment controls.

This could mean that depending on the design and structure of the tokenised deposits, bank depositors could have the fungibility between deposits and digital asset tokens within the DLT based network and its participating commercial banks. These digital asset tokens can then be traded or circulated between parties within the DLT network with the aim of:

- Efficient and lowered cost for real-time gross settlement on wholesale large value settlement.
- Original deposits may be held with the commercial banks, potentially lowering the risk to depositors as compared to other emerging forms of digital currencies.
- Utilisation of smart contract features, allowing self-execution and self-enforced policy, which is a major leap ahead of conventional deposits today.
- Tokens could be used as a form of value representation on the DLT network instead of the actual underlying deposits, unlocking additional liquidity for the commercial banks of the network.

Annex 3: Stablecoins

Stablecoins are tokens whose value is tied to another asset, usually fiat currencies such as the US dollar. Stablecoins are typically issued by non-deposit taking institutions and they seek to combine the credibility that comes from their supposed stability, with the benefits of tokenisation, that allow them to be used as payment instruments on distributed ledgers. Stablecoins can realise their potential only if there is confidence in their ability to maintain a stable value.

Many stablecoins lack the ability to uphold the promise of stability in their value. Some of the assets backing these stablecoins – such as commercial papers – are exposed to credit, market, and liquidity risks. There are currently no international standards on the quality of reserve assets backing stablecoins. Globally, regulators are looking to impose requirements such as secure reserve backing and timely redemption at par.

Depending on operational robustness and the safeguarding reserve's adequacy, stablecoins could be exposed to shortfall in its reserve leading to consumer fraud. This risk can be effectively mitigated by appropriate regulations. In this regard, jurisdictions globally, including in Singapore, are actively formulating a regulatory framework to regulate stablecoins with a view to ensuring that they can uphold the promise of stability in their value. Aspects of this include ensuring a suitable reserve asset composition to back the stablecoin, proper safeguarding of customer monies and consistent audits of stablecoin issuers' reserve backings.

Annex 4: Glossary of Terms

AML	Anti-Money Laundering
API	Application Programming Interface
CBDC	Central Bank Digital Currency
CDC	Community Development Council
CFT	Countering the Financing of Terrorism
DLT	Distributed Ledger Technology
ERC	Ethereum Request for Comments
FAST	Electronic funds transfer service
HSM	Hardware Security Module
MEPS+	MAS Electronic Payment System
NPO	Non-Profit Organisation
OGP	Open Government Products
PBM	Purpose-Bound Money
RTGS	Real Time Gross Settlement System
SFF	Singapore FinTech Festival
SGD	Singapore Dollar
TOP	Temporary Occupation Permit

This report is developed and published by Monetary Authority of Singapore with contributions from:

DBS Bank Ltd.
Grab Holdings Ltd.
Fazz Financial Group Pte. Ltd.
Network for Electronic Transfers (Singapore) Pte. Ltd.
OCBC Ltd.
Open Government Products
Temasek Holdings Ltd.
UOB Ltd.

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.

Monetary Authority of Singapore

PROJECT ORCHID

Copyright © Monetary Authority of Singapore

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanised, photocopying, recording or otherwise, without the prior written permission of the copyright owner.

Applications for the copyright owner's written permission to reproduce any part of this publication should be addressed to:

FinTech and Innovation Group (FTIG)
Monetary Authority of Singapore
10 Shenton Way MAS Building
Singapore 079117

November 2022