POINT-TO-POINT INTERBANK rCBDC FOR SINGAPORE AND BEYOND

Pralhad Dinesh Deshpande
Sanil Sinai Borkar

Table of Contents

Introduction

The evolution of Singapore's payment, clearing and settlement systems has been driven by technological progress. In this report, we highlight new technological progress, a brand-new way of transferring electronic value, that could significantly influence the design of retail Central Bank Digital Currency (rCBDC) infrastructure in Singapore and beyond.

We envision an electronic funds transfer system that allows customers to transfer rCBDC immediately between participating banks and non-financial institutions (NFIs). Unlike present day systems like Interbank GIRO (IBG) or Fast and Secure Transfers (FAST), our proposal allows for instant, point-to-point settlements with rCBDC. In our design there is no clearing phase. Each payment message is in fact a settlement message and is transferred point-to-point.

The proposed system operates with high integrity and is highly secure and resistant to insider attacks from malicious operators. It also enables continuous monitoring by a governing entity which also controls network membership. This opens the possibility for the proposed system to be operated by foreign banks and NFIs outside Singapore's jurisdiction while it's operations may be monitored by a Singaporean governing entity. This capability can expand the footprint of Singapore's rCBDC and give it global reach.

The proposed system does not have any central chokepoints and is capable of operating with unbounded throughputs. This opens up the possibility of enabling micro-payments. Over-the-Internet micro-payments, payments of fractions of cents, can unlock a whole new way of monetizing the web that does not rely on user surveillance for ad placement.

Our approach in this report is to first describe the current payment systems in Singapore with the objective of identifying gaps that can be filled with rCBDC. After that, we describe our technical innovation, the One Time Spend Machine (OTSM), which offers a different, point-to-point, approach to electronic value transfers. Several technical properties need to be jointly achieved in order to build the OTSM. We describe these in detail. On a humorous note, we also describe how not to build an OTSM. We continue the discussion by presenting our vision of rCBDC. We opine on how the rCBDC instrument may be designed, how it may be distributed to consumers, and what the infrastructure may look like. We also opine on the role that the regulator may play in enabling rCBDC. Apart from rCBDC, an OTSM network can also support the point-to-point transfers of several other financial instruments. We briefly describe these alternate use cases before offering our concluding remarks.

1. Domestic Interbank Retail Payments

We are interested in exploring how account to account domestic interbank retail payments happen in Singapore. For the purpose of this discussion we shall leave out cheque payments and focus on electronic value transfers.

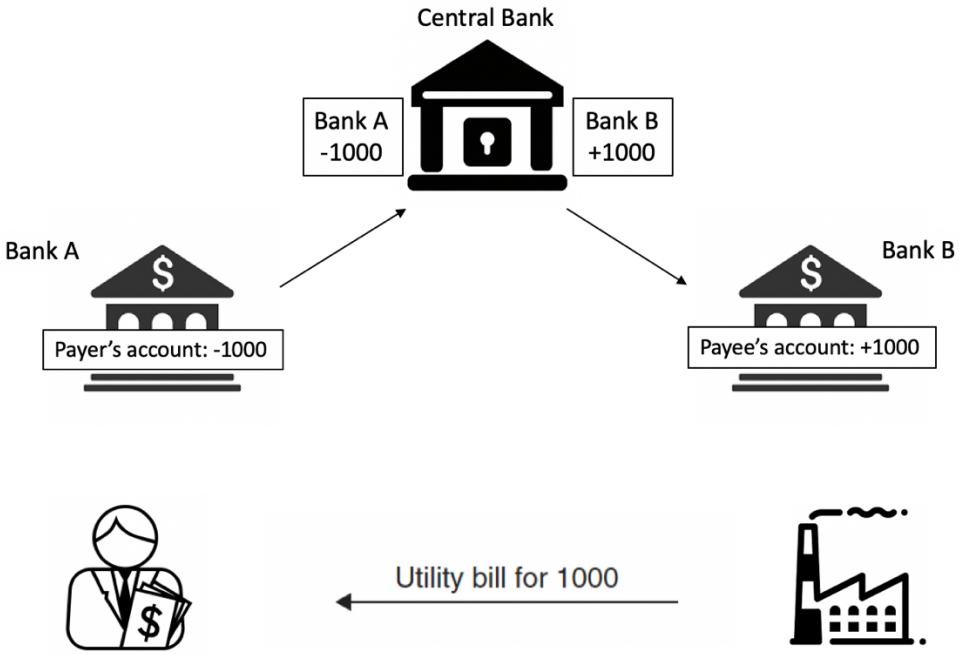

Figure 1: A naïve approach to interbank payments.

A naïve approach to interbank payments [1] is illustrated in Figure 1. The central bank plays the role of a settlement agent. Commercial banks maintain accounts with the settlement agent. Final and irrevocable settlement happens in 'central bank money' between accounts held at the central bank. This naïve approach does not work in practice because the payment volumes are too high.

1.1 Interbank GIRO (IBG)

The IBG system [2] is an offline interbank payment system catering to low-value bulk payments. IBG allows customers of participating banks to transfer funds to and from the accounts of customers of any other participating bank. Banks notify the Singapore Automated Clearing House (SACH) of payments to customers of other banks. The net settlement amounts for IBG transactions are sent by SACH to the new MAS Electronic Payment System (MEPS+), the RTGS system operated by MAS, for settlement at the end of day. The funds are made available to the customers of other banks after final and irrevocable settlement happens at MEPS+.

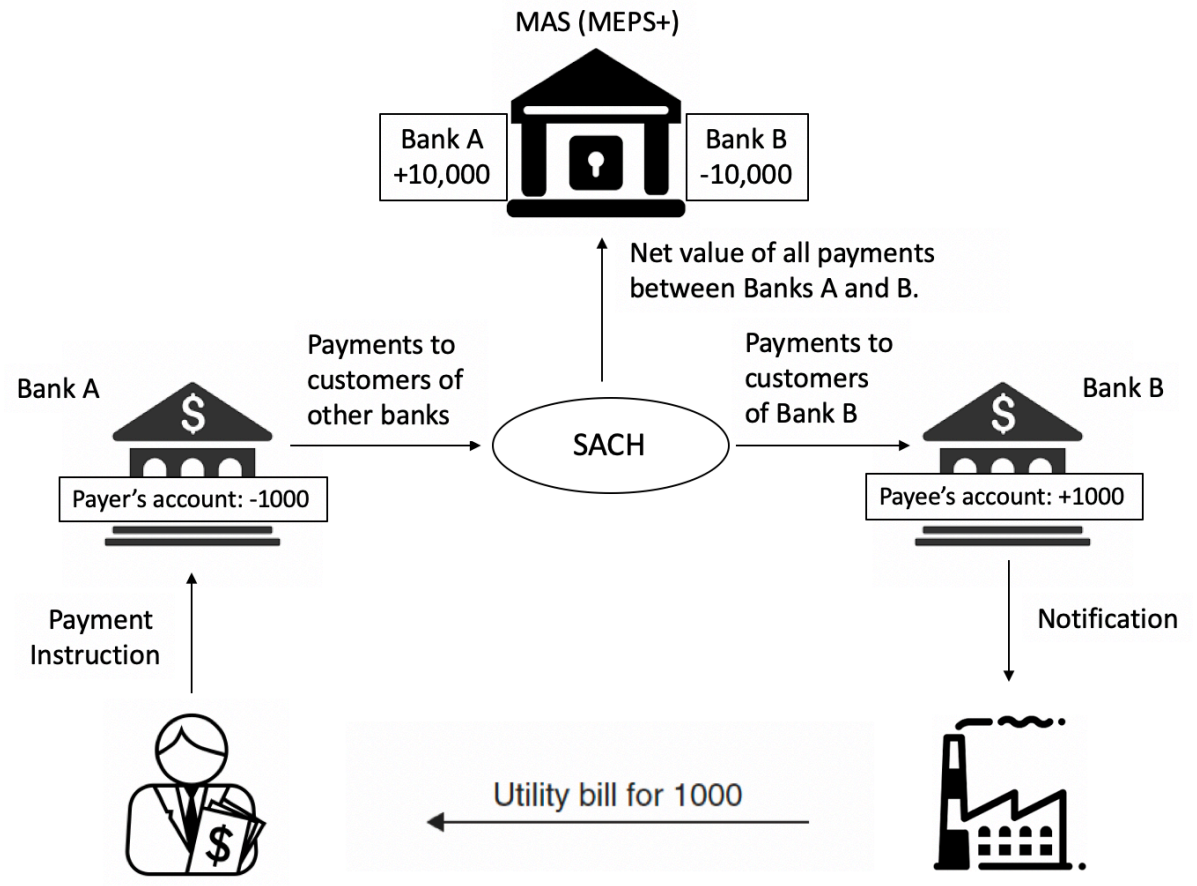

Figure 2: IBG clearing and settlement.

1.2 Fast and Secure Transfers (FAST)

FAST [3, 4] is an electronic funds transfer service that allows customers to transfer SGD funds almost immediately between accounts of 24 participant banks and 5 Non-Financial Institutions (NFIs). FAST operates 24x7x365.

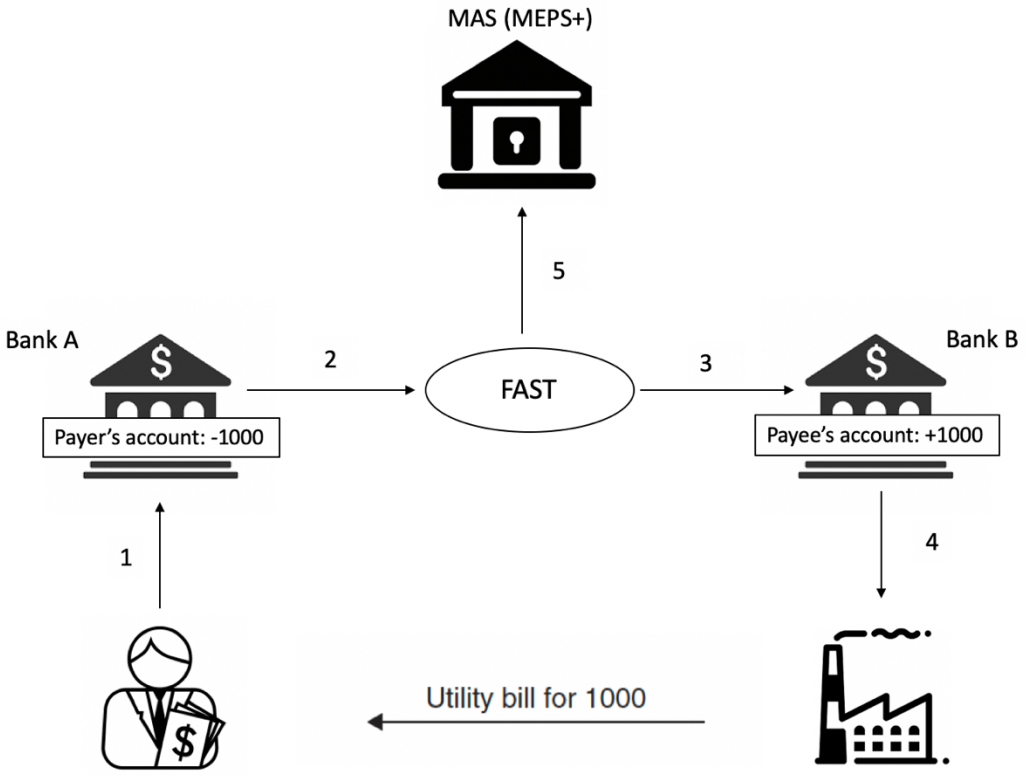

Figure 3: Payment flow for a FAST transaction.

The payment flow for a FAST transaction is as follows:

1. The payer initiates the funds transfer to the payee's bank account. The funds are debited immediately from the payer's bank account.
2. The payer bank sends the transaction to FAST for clearing.
3. FAST, which is operated by Banking Computer Services Pte. Ltd. (BCS), validates and routes the payments message to the payee bank.
4. The payee bank validates the bank account number and credits the payee's account immediately. The funds are available to the payee immediately.
5. FAST clearing obligations of all participating banks are transmitted by BCS to MEPS+ for interbank settlement on a multilateral net basis twice per working day.

As a point of difference from GIRO, funds transferred via FAST are immediately available to the recipient. This is achieved by the Payer Bank guaranteeing the transfer of funds and the Central Bank acting as the buck-stop, i.e., the Central Bank guarantees the fund transfer even if the Payer Bank defaults.

1.3 Gaps

1.3.1 Settlements are not Instant

Interbank settlements continue to be on a deferred basis following multilateral netting. The default of any bank can lead to not meeting its payment obligations and can lead to large systemic risks that can impact several banks.

1.3.2 SGD Usage Outside Singapore has Frictions

The footprint of SGD is primarily limited to Singapore. There are good reasons to believe that expanding the frictionless availability and use of SGD beyond Singapore can lead to several benefits [5]. If we can make SGD the most frictionless currency to be used for cross-border trade, it will significantly drive the foreign demand for SGD and lead to magnified foreign currency inflows.

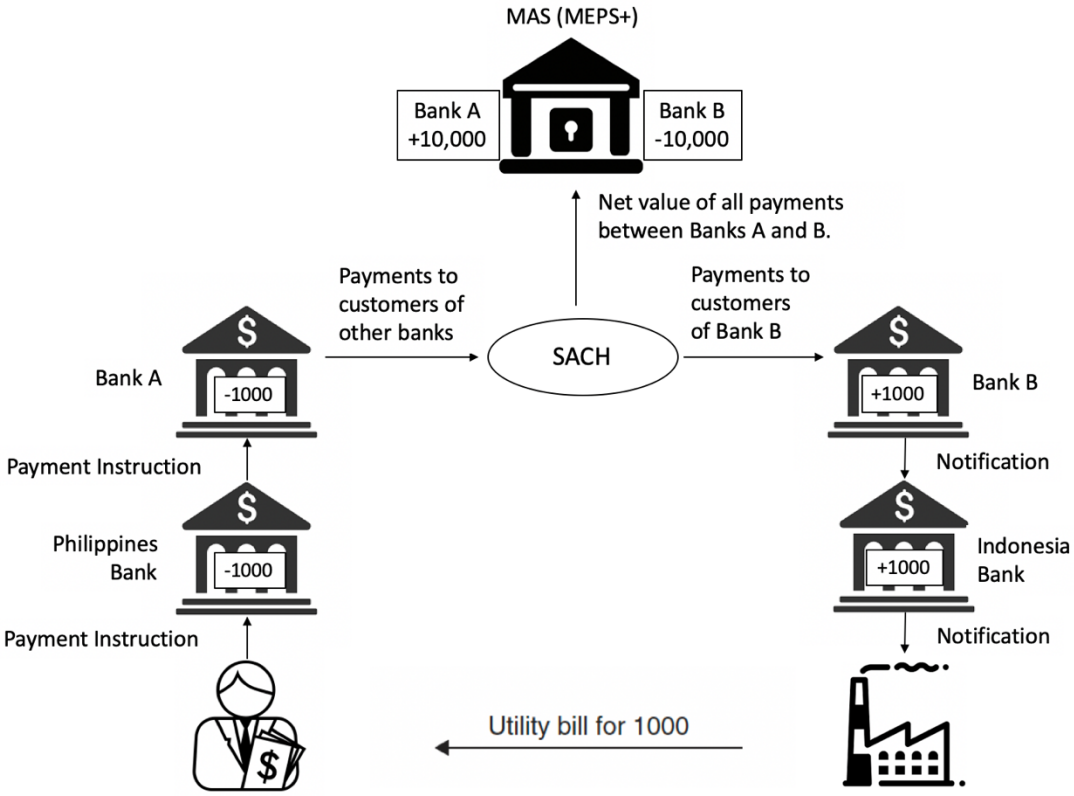

Figure 4: SGD use outside Singapore has many friction points.

Consider a scenario where a payer in the Philippines wants to pay someone in Indonesia with SGD. The transaction would flow as illustrated in Figure 4. Each hop adds delay. Each hop also incurs fees.

A reduction in these friction points can unlock the use of SGD in cross-border payments. Note: cross-border payments do not necessarily have to be cross-currency payments. A payee could convert SGD to local currency on demand by trading it in the local currency market or continue to pay with it onward.

1.3.3 Micro-payments are not Possible

The proliferation of the web was fueled by the discovery that it offered an excellent medium for targeted advertising. Targeted advertisements have led to a surveillance economy. The surveillance economy offers very severe privacy concerns to individuals. While privacy related

regulations can go a long way to address this problem, it has been considered for a long time that the antidote to surveillance capitalism is micro-payments. Micro-payments are over-the-Internet payments with fractions of cents. Unfortunately, the current payment systems in Singapore and beyond do not support micro-payments.

1.4 Summary

Payment systems in Singapore are designed to facilitate frictionless payments within the national boundary. Even so, they continue to be susceptible to bank defaults that may lead to systemic risks. Modern day payment systems also do not support micro-payments. In designing systems to support rCBDC, it would be apt to focus on addressing these gaps in modern day payment systems.

2. One Time Spend Machine (OTSM) – A Technical Innovation

In this section, we elaborate on the technical innovation that we bring to the table. We propose a new electronic value transfer system that facilitates point-to-point interbank electronic value transfers.

2.1 Basic Concept: Settlement Across Two Ledgers

Until now, settlements have always been thought of as happening within the context of a single ledger or database. The ledger is either maintained by a single settlement agency or a group of entities. An example of the former is the ledger (or database) maintained by MAS's MEPS+ system. Final and irrevocable settlements of interbank payments only happen here. An example of the latter is the Bitcoin blockchain which is operated by a changing set of 'miners'. This distributed ledger, because of the consensus algorithm employed, only allows for probabilistic settlements instead of final and irrevocable settlements.

We propose a departure from the single ledger concept. Imagine two banks, each maintaining their own databases with customer accounts and balances.

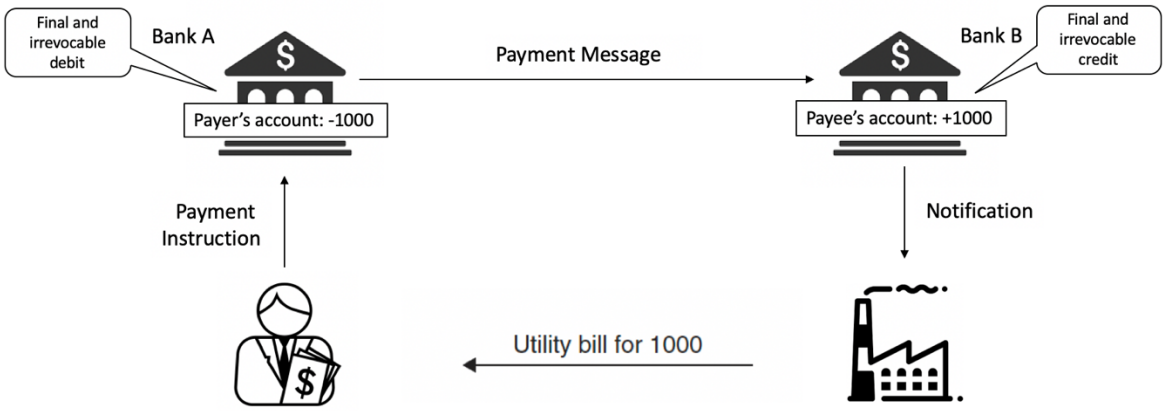

Figure 5: Point-to-point transfers

Now imagine that a payment instruction from Bank A's customer can cause a final and irrevocable debit at Bank A. As an output of the debit process, a payment message with Bank B's customer as the payee is generated. The payment message is sent to Bank B where a final and irrevocable credit is performed. This final and irrevocable debit, payment message transfer and final and irrevocable credit can jointly be viewed as the settlement process.

2.2 Digital Bearer Assets (DBA)

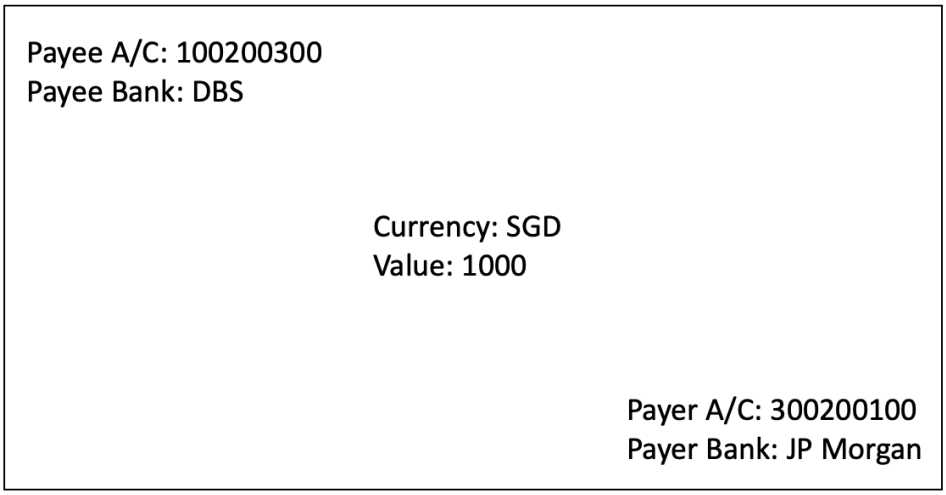

Figure 6: Fungible Digital Bearer Asset

We call the payment message that is generated as an output of the final and irrevocable debit process a digital bearer asset (DBA). In the current context, it is a fungible DBA.

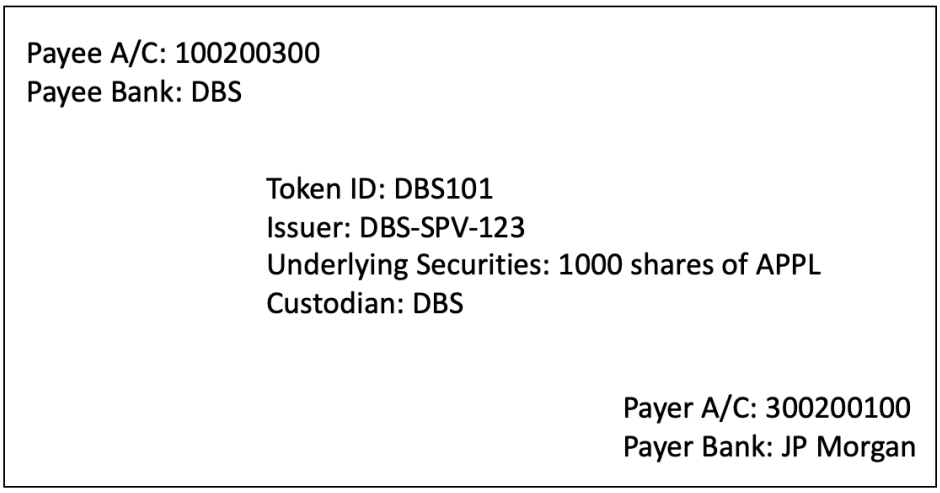

Figure 7: Non-Fungible Digital Bearer Asset

It is also possible to transfer non-fungible DBAs between banks. These may represent ownership titles to tokenized real estate or securities that may be issued using Special Purpose Vehicles (SPVs) where the underlying asset is maintained as a custodian.

2.3 Final and Irrevocable Debit

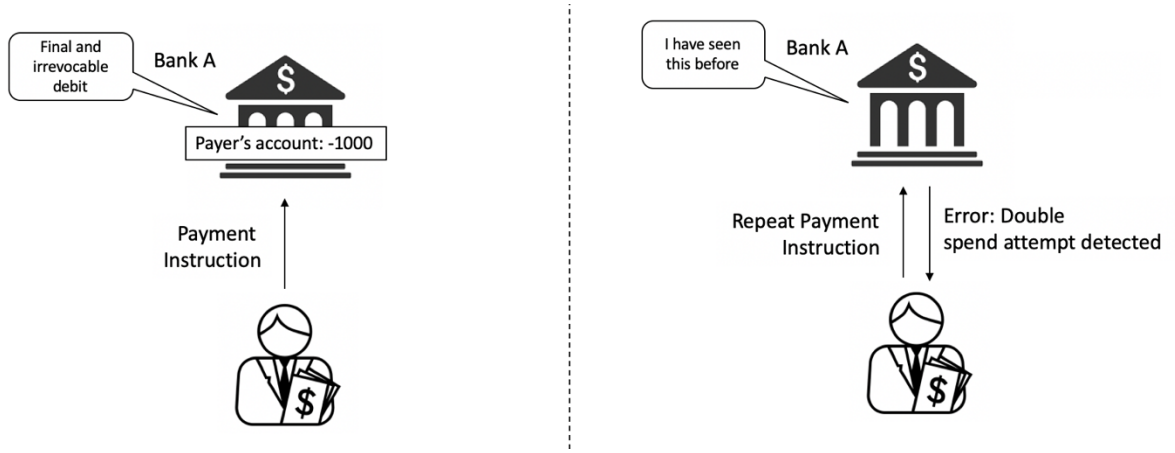

Figure 8: Final and irrevocable debit.

The main technical challenge in implementing final and irrevocable debit is to ensure that the same payment instruction is not processed multiple times. Our product, OTSM, guarantees that a payment instruction is processed only and only one time.

2.4 Final and Irrevocable Credit

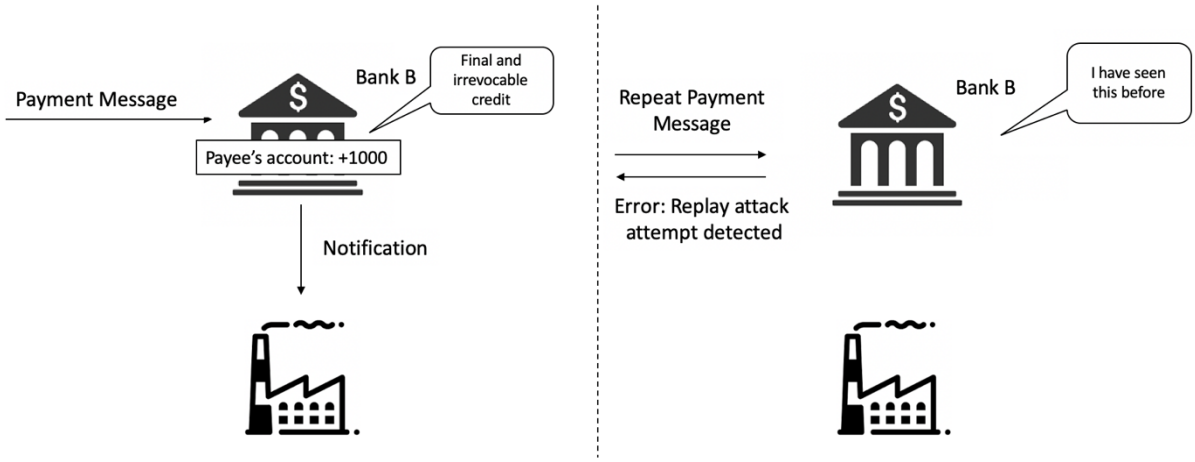

Figure 9: Final and irrevocable credit.

The main technical challenge in implementing final and irrevocable credit is to ensure that the same payment message is not processed multiple times. Our product, OTSM, guarantees that a payment message is processed only and only one time.

2.5 How not to Build an OTSM

We now describe a naïve approach towards building an OTSM. This is simply to bring out the core concepts. We emphasize that this is not how a practical system should be implemented.

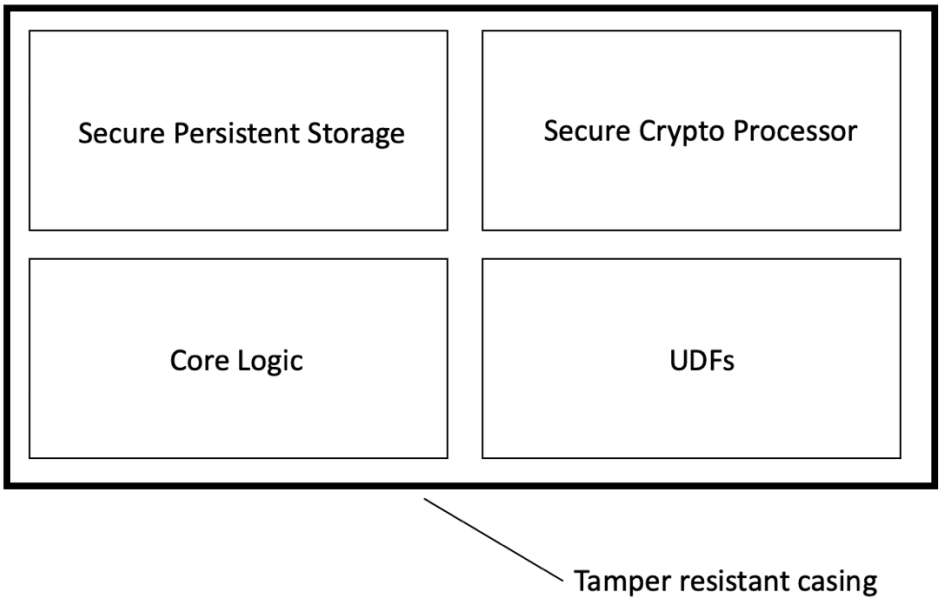

Figure 10: Logical view of a Hardware Security Module (HSM).

Let us start by using a commodity HSM. HSMs are very commonly used in the payments industry for the secure generation, storage and use of cryptographic keys. They are resistant to insider attacks. The hardware casing ensures that any attempts to open it to gain access to the components inside results in permanent destruction of the root keys making the HSM useless.

In addition to ensuring secure cryptographic operations, HSMs also allow administrators to develop and load custom logic in the form of User Defined Functions (UDFs) into the HSM. HSMs guarantee the secure execution of UDFs. HSMs also have the ability to securely store data in a persistent manner.

Now imagine that a custom UDF is written to process a payment instruction only one time. The UDF would leverage the secure persistent storage to store the signature of every payment instruction that it processes. Before processing a new payment instruction, the UDF would search for the signature of the payment instruction in the secure storage. If a signature is found, it means that the HSM has processed this transaction before and would revert with an error. If on the other hand, a signature is not found, the HSM will process the payment instruction by performing a final and irrevocable debit, adding the signature to the secure storage, and outputting a payment message to be transferred to the payee's bank.

There are two problems in this approach.

Problem 1: The secure persistent storage within HSMs is very limited. Often it is as low as 4 MB. This means that if OTSM were designed in this way, it would run out of storage after only a few seconds of continuous use.

Problem 2: The secure persistent storage is not replicated. If the HSM stops functioning, we have no recall of previous transactions.

Our product, OTSM, overcomes these challenges. It can operate continuously without running out of storage. It is also resilient to node failures.

2.6 Flexible Resilience

OTSM offers flexible resilience based on customer requirements.

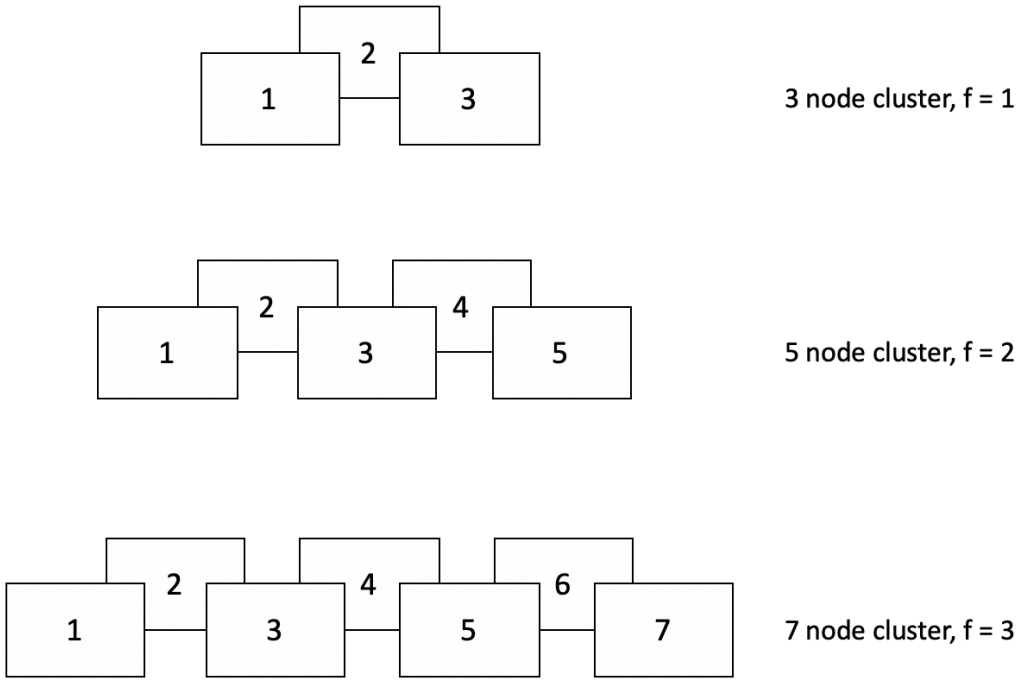

Figure 11: OTSM offers flexible resilience.

OTSM operates as a cluster of nodes. A cluster of n nodes offers tolerance to f faults where, n = 2f + 1. Also, the cluster nodes can be geographically distributed ensuring that disaster recovery protocols can be properly implemented.

2.7 Scalability

2.7.1 Single Site Scalability

OTSM allows transaction processing to be parallelized across multiple cluster nodes.

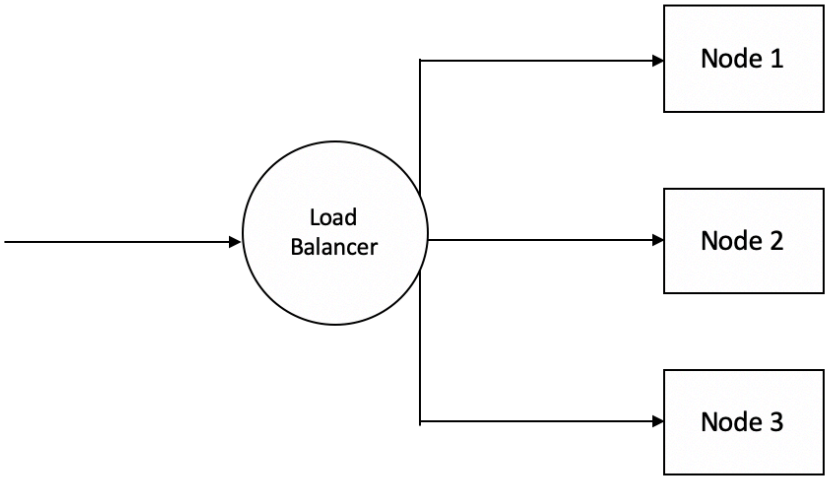

Figure 12: Transactions can be processed in parallel. Add more nodes for more throughput.

Thousands of transactions per second can be processed and the cluster size can be expanded to support increasing throughput requirements.

2.7.2 Network Scalability

Our design allows network throughputs to scale with new deployments. Since transactions do not flow through a single bottleneck there is no upper bound to network throughputs.

3. rCBDC

3.1 Instrument

3.1.1 rCBDC as a fungible DBA

We believe that rCBDC maps well to the concept of a fungible DBA. Discretization of values, e.g., by using non-fungible DBAs to map to various currency denominations adds complexity to the process of electronic value transfers and should be avoided when possible.

3.2 Distribution

3.2.1 Minting

Before looking into how rCBDC may be distributed, it is important to consider how it could be securely minted. We believe the best approach is to establish a multi-level hierarchical structure within the minting entity so that new rCBDC may only be generated with the consent of the approval chain.

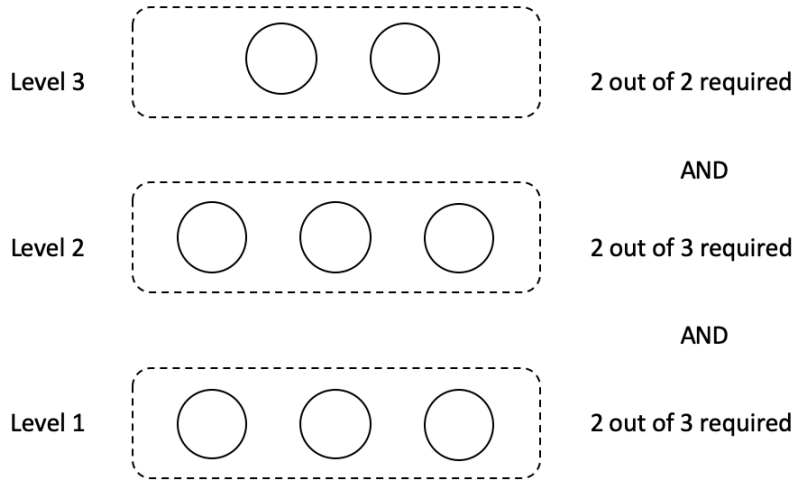

Figure 13: A hierarchical approval chain for minting rCBDC.

OTSM allows the establishment of a hierarchical structure for the rCBDC minting process. It is possible to set rules as illustrated in Figure 13. As shown in the figure, new rCBDC will only be minted if the mint request is approved by 2 out of 3 administrators at level 1, 2 out of 3 administrators at level 2 and both administrators at level 3.

3.2.2 rCBDC Stored Value Facility (SVF)

Our view is that banks and NFIs offering rCBDC to their customers can operate a Stored Value Facility where the value stored is in rCBDC.

3.2.3 Access Channels

Customers may be able to access their rCBDC accounts with a multitude of access channels including telephone banking, mobile banking, Internet banking, and via self-service machines.

3.3 Infrastructure

In this section, we shall incrementally develop the infrastructure needed to support rCBDC.

3.3.1 rCBDC SVF Network

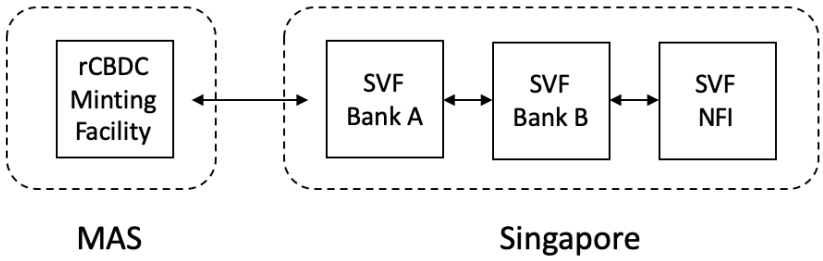

Figure 14: An rCBDC SVF network in Singapore.

As described earlier, rCBDC should be minted within a minting facility maintained by MAS. Banks may operate SVFs where the stored value is in the form of rCBDC. rCBDC is maintained as account balances for the bank's customers. Figure 14 shows a set of Singaporean banks offering rCBDC to their customers. Interbank transfers can happen in a peer-to-peer fashion.

3.3.2 Expanding beyond Singapore

Domestic retail payments within Singapore are quite fast and convenient. They are also done at zero cost to customers. The real value of rCBDC lies in unlocking cross-border payments.

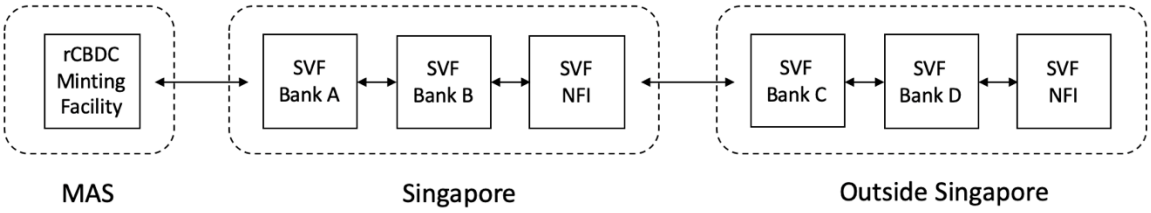

Figure 15: An rCBDC SVF network spanning outside Singapore.

Figure 15 shows a scenario where banks outside of Singapore also operate rCBDC SVFs. rCBDC can conveniently flow between any two banks in the rCBDC network.

3.3.3 Monitoring

If rCBDC is to flow over a direct link between banks, then how can a central monitoring agency tasked with AML and CTF objectives perform its function?

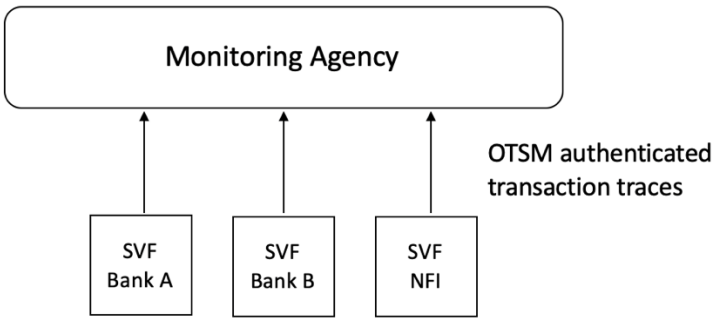

Figure 16: Interbank Messaging and Transaction Monitoring.

The approach that we suggest is for each rCBDC SVF to upload an OTSM authenticated trace of transactions to a central monitoring agency which may be appointed by MAS. A trace may be uploaded at the end of every day.

3.3.4 Membership Control

A governing entity also needs to be able to control the membership of rCBDC SVFs within the network. Adding and removing members should be convenient.

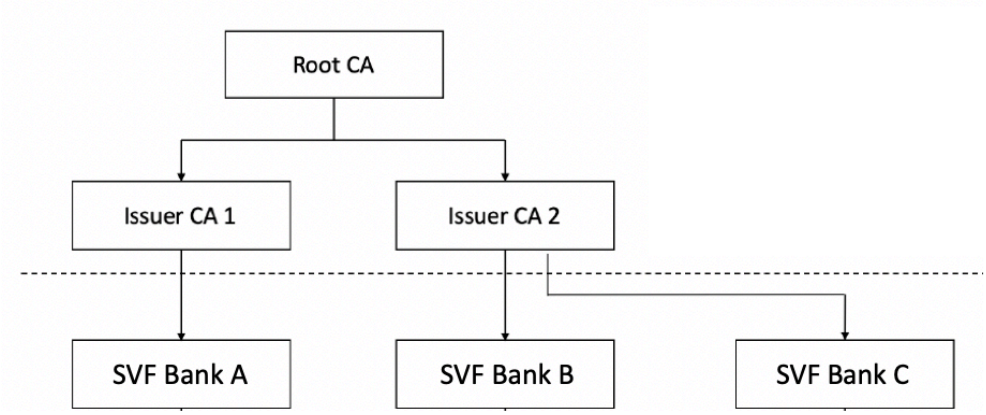

Figure 17: Membership Control.

As shown in Figure 17, Certificate Authorities (CAs) may be established to issue and revoke certificates to individual SVFs. If it is observed that an SVF is not obeying membership rules, their membership certificate may be revoked and this would prevent them from transacting with any other SVFs in the network.

3.4 Role of Monetary Authority of Singapore (MAS)

Before establishing the role of MAS in the proposed model, it is important to highlight the roles that will not be played by MAS. MAS will no longer play the role of a settlement agency. It will not operate a central settlement system such as MEPS+ to settle rCBDC transactions.

3.4.1 Issuer

MAS or an agency appointed by it will play the role of rCBDC issuer. As described above, OTSM provides mechanisms for secure issuance of rCBDC.

3.4.2 Overseer

MAS will continue to be an overseer of the network with the objectives of ensuring safety and efficiency. Also, MAS will be in charge of membership control of the rCBDC SVF network.

4. Beyond rCBDC

Imagine the deployment of an OTSM network across various banks and NFIs. The network supports the final and irrevocable transfers of both fungible and non-fungible DBAs. Beyond rCBDC, several other types of financial assets can flow through this network.

4.1 Bank Issued Fiat backed Digital Currencies

Banks could issue their own fiat backed digital currencies in various denominations. The same network can support the transfer of several currencies. As in the case of rCBDC, the issuer can monitor the transactions and also perform membership control.

4.2 Secondary Market for Tokenized Loans

Often, banks engage in simple interbank agreements to be able to transfer the risks associated with loans. Consider funded participation for instance. These bespoke agreements are hard to manage. Instead, if loans could be captured as non-fungible DBAs, then they could easily be transferred from bank to bank. This could create an OTC market for secondary loans.

4.3 Tokenized Collateral Transfer for Interbank Repo

Consider the interbank repo market. Often banks want short term cash and have to hand over collateral to the other bank in return of this cash. Cash flows at much faster speeds than collateral. Collateral settlements often happen over a T+2 or T+3 settlement cycle. If collateral is tokenized, it could be transferred between banks instantly. This could bring considerable efficiencies in the interbank repo markets.

5. Conclusions

The domestic retail payments system in Singapore is very efficient. It offers real time and zero cost interbank account to account transfers to bank customers. Nonetheless, even though payments are almost instant, interbank settlements continue to be deferred to the end of day or twice daily. Also, while dealing in SGD is convenient in Singapore, it is not a convenient instrument outside of Singapore. Finally, the current payment system does not support micro-payments. Enabling micro-payments could unlock new ways for web-monetization and could lead to significant societal benefits. In designing rCBDC, it is important to address these gaps in the current payments system in Singapore.

Technological advancements have led to improvements in the payments systems in Singapore. In this report, we have highlighted a new technical development – a technology that can enable instant bank-to-bank settlements using rCBDC. Our technology can be deployed to address gaps in present-day payments systems.

6. References

[1] Payment Systems – From the Salt Mines to the Board Room. Rambure, D., Nacamuli, A.

[2] Payment, Clearing and Settlement Systems in Singapore. EMEAP – Red Book – 2011. [URL]

[3] Fast and Secure Transfers – Fact Sheet [URL]

[4] Fast Payments – Enhancing the speed and availability of retail payments. [URL]

[5] YouTube: Digital Currency Series (Part 1): 'Live' Adoption – what's next? | The Green Shoots Series 2021. [URL]