Three principles guiding the design of the HKMA's proposed retail central bank digital currency architecture

Hong Kong Monetary Authority (HKMA)

About this paper

This paper aims to offer meeting participants an overview of the HKMA's retail central bank digital currency (rCBDC) study as well as to highlight three selected principles that guided our design of the proposed architecture. The first section of the paper provides a background of the e-Hong Kong dollar (e-HKD) study being conducted by the HKMA, in which an architecture for distributing and circulating rCBDC was proposed. The second section briefly discusses the model adopted, explains why it was chosen, and describes how the architecture works. The third and final section delves into three of the design principles that were considered by the HKMA over the course of devising the proposed architecture, namely flexibility, privacy-preserving ability and interoperability.

1. Background of the HKMA's e-HKD study

In June 2021, the HKMA commenced Project e-HKD, a feasibility study on rCBDC and digitisation of the Hong Kong dollar to increase the city's readiness for issuing rCBDC if it decides to do so in the future. The project consists of two parts. The first part is a technology experimentation study which investigates the infrastructure needed for issuing and distributing rCBDC. Specifically, it examines how certain commonly recognised issues relating to rCBDC can be addressed or mitigated through suitable architectures and designs. The second part is a comprehensive study of other issues pertaining to the feasibility of issuing e-HKD, covering use cases, benefits, legal and monetary considerations, and risks related to data privacy, anti-money laundering (AML) and cyber security.

As part of the technology experimentation study, in October 2021 the HKMA published a technical white paper which reports the initial thoughts and findings on the potential architectures and design options that could be applied to the construction of the e-HKD distribution infrastructure. An architecture was proposed in the white paper, and comments and suggestions from the industry and academia were solicited.

While a conclusion regarding issuing e-HKD has not been reached, the HKMA remains open-minded on the matter, and aims to formulate a stance and offer its initial thoughts in the middle of 2022.

2. Overview of the proposed architecture

The two-tier model, in contrast to the one-tier/direct model, was adopted in the HKMA's proposed architecture. The rationale behind this decision will be discussed only briefly given that the merits (as well as drawbacks) of the two-tier model have already been discussed at length in various papers published by the BIS.

In brief, the two-tier model was chosen for the proposed design because it could preserve the division of labour between the central bank and private sector intermediaries, ie commercial banks and payment service providers (PSPs), implying that the central bank can focus on providing the core infrastructure, and delegate the majority of customer-facing activities and operational tasks to the intermediaries. Another particular strength of a two-tier model is its capability to decouple the wholesale and retail layer, ensuring that cyber attacks originating in the retail layer will not be cascaded into the wholesale one, resulting in a more cyber-resilient CBDC system overall.

The HKMA's proposed architecture consists of two layers. The first layer, which is the wholesale system, is where wholesale CBDC (wCBDC) issuance and redemption take place, and is only accessible to the central bank and intermediaries. Its distributed ledger technology (DLT)-based nature enables intermediaries to settle interbank payments among themselves without involving the central bank. The second layer is a retail system for distributing and circulating rCBDC. It is operated by the intermediaries and is accessible to general users who are equipped with mobile wallet applications. Between the wholesale and retail system are the intermediaries who act as a bridge to facilitate communication and synchronisation between the two systems. Most importantly, a mechanism is present in the architecture to ensure that every rCBDC distributed in the retail system is backed by wCBDC in the wholesale system in a verifiable manner at all times. This mechanism eliminates the problem of over-issuance of rCBDC.

In the retail system, the distribution and circulation of rCBDC is based on the unspent transaction outputs (UTXO) model. By nature, UTXO enables traceability of transactions by embedding a chain of records of previous transactions. Features to address the privacy concerns of UTXO will be discussed in Section 3.2. Another notable feature is the presence of the validator infrastructure.[1] It is responsible for verifying every retail payment transaction so as to prevent the problem of double-spending, ie spending the same rCBDC more than once.

3. Three principles guiding the design of the proposed architecture

Over the course of devising the proposed architecture, the HKMA considered a number of design principles. With reference to the meeting agenda, three of these

[1] For details about the validator infrastructure, such as its design and implementation, please refer to the HKMA's technical white paper, e-HKD: A technical perspective (www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/e-HKD_A_technical_perspective.pdf).

principles, namely **flexibility**, **privacy-preserving ability** and **interoperability**, were selected and will be discussed below.

3.1 Flexibility

The HKMA is of the view that, to maximise the usability of any design of CBDC issuance and distribution infrastructure, the infrastructure should ideally be based on a flexible architecture, so that central banks are allowed a certain degree of flexibility to implement different two-tier models according to their respective jurisdictional contexts, and to accommodate changes as informed by new policy research findings. Ideally, the design should be reconfigurable so that by configuring different components of the system, different two-tier distribution models can be achieved.

The HKMA's proposed architecture is designed with flexibility in mind. First of all, the adoption of the two-tier model implies that the design of the wholesale and retail systems could be made independent. For example, currently the wholesale system is based on DLT. In the event that a centralised database similar to the real-time gross settlement (RTGS) system is preferred to suit the local context, this change in preference in the wholesale system would have minimum impact on the design of the retail system.

The design of the retail system further demonstrates the flexibility of the proposed architecture. For instance, the validator infrastructure can be configured to achieve different two-tier models. If the host of the validator infrastructure is the central bank, a hybrid CBDC model can be achieved. If the validator infrastructure is hosted by a designated joint venture of all the intermediaries, an intermediated CBDC model can be achieved. The usability of an infrastructure based on such a flexible architecture would be greatly maximised.

3.2 Privacy-preserving ability

User privacy is commonly regarded as one of the most valued properties and key success factors that determine whether an rCBDC would be generally accepted and used by the general public. Thus it is natural to include privacy-preserving elements in the design of the proposed architecture. This section briefly explains how the HKMA's proposal could preserve a user's privacy on two fronts: first, by limiting the central bank's access to retail payment data; and second, by restricting access to a user's information to that user's bank only, ie not allowing other users, or intermediaries of which the user is not a client ("non-client intermediaries"), to access the user's information.

First, limiting the central bank's access to retail payment data is made possible by the flexible nature of the proposed architecture. As pointed out in Section 3.1, in the proposed architecture, the validator infrastructure can be configured to achieve different two-tier models. If the validator infrastructure in the retail system is operated by intermediaries, the role of verifying the retail payment transactions and maintaining the retail balances is assumed by the intermediaries, not the central bank. As the central bank is not present in the retail system at all, it has no access to individual users' retail payment data, thus users' privacy can be preserved.

Second, preservation of user privacy vis-à-vis other users and non-client intermediaries could be made possible by a pseudonym system. While the natural transaction traceability of a UTXO model allows intermediaries and users to know who

held the rCBDC in the past, such traceability would have privacy implications. To address this issue, the proposed architecture explores the possibility of creating pseudonyms, similar to "nicknames", to represent the transacting parties during each and every transaction. Only a user's bank has access to the mapping between the pseudonyms and the user's real identity, which means that only a user's bank, not other users or intermediaries, knows the real identity of an rCBDC owner.

3.3 Interoperability

In the context of a two-tier model, a CBDC infrastructure should ideally be designed in a manner that allows interoperability between systems of different banks and PSPs. In other words, customers of different banks and PSPs should be allowed to make CBDC payments freely between themselves, in contrast to only permitting CBDC payments between customers of the same provider, ie a closed-loop payment system. In the HKMA's proposed architecture, intermediaries would use the same set of standards for communication in the retail system, allowing banks, PSPs, and their systems to better interconnect with each other. This arrangement would enable rCBDC retail payments to flow across different intermediaries seamlessly.

In addition, to support overseas users or wallets, ie cross-border transactions, the CBDC infrastructure should preferably be designed in a way that allows extension of services and functionalities in order to support interoperability with other jurisdictions' CBDC systems in the future. In the proposed architecture, due to cyber security and resilience considerations, by design users would need to initiate transactions through their banks or PSPs, instead of accessing the validator infrastructure directly; and the same principle applies to overseas users. To support cross-border interoperability, there is a dedicated structure in the proposed architecture with a role similar to that of a service provider, for overseas users to connect to the validator infrastructure and make CBDC payments.

Closing

This paper has briefly discussed three design principles considered by the HKMA during the course of devising the proposed architecture, namely flexibility, privacy-preserving ability and interoperability; but they are by no means the only principles examined. The HKMA hopes that the principles highlighted in the paper will spark an exchange of views and facilitate a fruitful discussion among participating central banks. More in-depth explanation of the proposed architecture is provided in the HKMA's technical white paper *e-HKD: A technical perspective*, downloadable from the HKMA website.