FINTECH ASSOCIATION OF HONG KONG

HKMA's e-HKD Technical Whitepaper on Retail Central Bank Digital Currency

FTAHK Consultation Response

CONTENTS

The FinTech Association of Hong Kong (FTAHK) is a **member-driven, independent, not-for-profit, & diverse** organisation that is the voice of the FinTech community in Hong Kong. It is organised and led by the community, for the community, through a series of committees and working groups.

Our objective is to promote Advocacy, Communication and Education in the wider FinTech ecosystem.

Build the community.

Be the connector.

A. FOREWORD

The Hong Kong Monetary Authority (HKMA) released on the 4th October 2021[1] a technical whitepaper on retail central bank digital currency (CBDC), titled "e-HKD: A technical perspective"[2].

As part of HKMA's "Fintech 2025" strategy announced in June 2021, one strategic direction is in the area of future-proofing Hong Kong in terms of CBDC readiness, including a study on the prospect of issuing retail CBDC in Hong Kong.

The HKMA indicated that the *e-HKD: A technical perspective* paper was developed with the Hong Kong Centre of the BIS Innovation Hub. The paper presents a preliminary analysis of a proposed architecture and the HKMA has invited comments on seven problem statements as well as soliciting new ideas and proposals related to them. The HKMA has also invited comments on the security modelling and analysis for the proposed design, as well as ideas for novel use cases and capability that can be uniquely enabled by rCBDC.

Please note, that while we have consulted widely, any views expressed in this submission are the views of FTAHK and do not necessarily represent the views of individual contributors or Members.

We offer our thanks on behalf of the FTAHK's Digital Banking & Payments Committee, the FTAHK's Blockchain Committee, and the Board of Directors. The FTAHK welcomes the opportunity to discuss any of the feedback provided in future follow up sessions with HKMA, The Hong Kong Centre of the BIS Innovation Hub, and relevant stakeholders.

FTAHK

31st December 2021

https://ftahk.org admin@ftahk.org

[1] https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/10/20211004-3/

[2] https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/e-HKD_A_technical_perspective.pdf

B. THEMATIC FEEDBACK

B.1 TARGETED SCOPE OF RETAIL e-HKD FOR TECHNICAL ASSESSMENT - 'LEGAL TENDER NOTES AND COINS' OR BROADER?

In order to identify the appropriate technical features of a future e-HKD system, clarification of the scope of the target market to be addressed in the ranges of 'money' and payments will be essential for ensuring fit-for-purpose capabilities

A clear definition of the targeted scope of the retail e-HKD is needed for a technical assessment. The scope could range from the narrowest 'legal tender notes and coins' or elements of the retail payment or stored value systems that access demand deposit accounts with the licensed banks (see Appendix 1 for analysis of the Money Supply and associated scale of retail payment systems in Hong Kong).

Consideration should be given to the breadth of future needs, as the extent to which an e-HKD system would replace commercial bank money (rather than currency) has significant technical and operational considerations.

B.2 FUNCTIONAL REQUIREMENTS IN CONTEXT OF CURRENCY IN THE HONG KONG S.A.R, PRC

The role of wholesale e-HKD to provide trust in the retail e-HKD appears to overstate this need, which is currently addressed through the Currency Board and understate the other potential roles of wholesale e-HKD.

The issuance and operation of currency in Hong Kong differs from a large number of territories and countries as it is primarily undertaken by private commercial banks. At the end of 2020, private bank issued currency accounted for approximately 90% of the notes by volume and 99.5% of the notes by value. The Government currently only issues the lowest value note (HKD10) and coins. The private bank-issued notes are fully backed by USDs deposited in the Exchange Fund in return for zero interest certificates of deposit (indebtedness). This Currency Board arrangement has provided confidence in the current HKD currency, which at the end of 2020 was HKD559bn. See Appendix 1 for further details.

Whilst the e-HKD technical perspective paper covers both 'wholesale' and 'retail' CBDC, it is not clear that the full range of needs that the wholesale e-HKD CBDC could address have been considered.

The paper appears to assume it is necessary to provide trust in the retail CBDC, however as the current private bank issuance of legal tender notes indicates, the existing Currency Board arrangement (full USD backing of the notes) is providing confidence sufficient for the value in issue.

If the wholesale CBDC is only for support of the retail, the cost/benefit would appear to be difficult to justify.

If, however, the wholesale CBDC has the intention to address other needs, for example cross-boundary or cross-border, as being considered by the mBridge pilot phases, these will have a significant impact as part of the technical requirements.

The functional requirements of the technical aspects of the e-HKD will need to complement the existing system, which has a level of flexibility already with both private commercial bank and Government issued currency. This provides a basis for considering the e-HKD as an opportunity based on policy objectives to evolve the currency, for example to adjust the balance of Government issued currency to private issue currency, or for adjusting the backing of the currency. Such functional requirements will have an overriding impact on the application of the technical system, for instance whether a single entity or multiple entities are responsible for originating currency.

B.3 'BEARER' OR 'ACCOUNT' BASED E-HKD AND THE LIABILITY FOR COUNTERFEIT

After considering the targeted scope (B.1) and the context (B.2) , one of the most significant decisions that will impact the technical design will be the extent to which the e-HKD is a bearer instrument and the allocation of liability for counterfeit.

Physical banknotes are 'bearer' instruments. The bearer is the owner of the value represented by the note. If the bearer misplaces the note, for example it is dropped, stolen, or physically destroyed, the bearer loses the value.

The bearer also accepts the loss if the receiver is able to detect the note as a counterfeit and then refuses to accept the note. The chain of detection passes from the holder to the receiver to the bank accepting the note, to the note issuing bank if a bank returns a note to the note issuing bank and in the case of return notes to the central bank, to the central bank if the central bank accepts the note.

A core feature of currency as legal tender is that the holder does not bear the credit risk of the institution as the money is accepted by any of the regulated banks, supported in Hong Kong by the Exchange Fund.

This is in contrast to either stored value issued by a regulated stored value facility in Hong Kong or money denominated in commercial bank accounts, where the owner is exposed to the credit risk of the institution, although in the case of commercial bank accounts there is mitigation through the Hong Kong Deposit Protection Scheme up to HKD0.5m per eligible account per Scheme member.

After considering the context and the targeted scope, one of the most significant decisions that will impact the technical design will be the extent to which the e-HKD is a bearer instrument and the allocation of liability for counterfeit.

B.4 CENTRAL ROLE OF TRUSTED EXECUTION ENVIRONMENTS (HARDWARE SECURITY MODULES/SMARTCARDS) FOR CRYPTOGRAPHICALLY CRITICAL FUNCTIONS

The cryptographic operations necessary to meet the scaled functional objectives of the e-HKD scheme will need to utilise Hardware Security Modules ('HSM') or equivalent to protect cryptographically critical functions such as private key storage

Private key storage

The technical perspective paper would benefit from considering the role of trusted execution environments, for example HSMs. smart cards, TEE within smart phones for cryptographically critical functions such as private key storage combined with the performance and scaling objectives of the scheme.

Consideration should be given to incorporating HSMs as part of the backbone of security as part of the hardware infrastructure required for a CBDC, for example a cluster of HSMs could be used to secure the central bank's private key used to issue a wholesale CBDC.

Offline capabilities

A number of assessments of retail CBDC, including the expanding pilot in mainland China identify the critical need to address the ability for offline transfer as a feature of the system (within controls and limits), rather than a 'fallback' in case of outages as the paper indicates in Section 6 of Table 1 on page 3.

Offline capability as a requirement is likely to necessitate the incorporation in the system of readily available tamper resistant cryptographic key stores and processing (commonly referred to as 'Trusted Execution Environments (TEE)' and usually relying on hardware based smart card technology at a sufficient level of assurance) on either 'chip cards' or TEE within smartphones or similar consumer devices.

The HKMA has previous experience through regulating smart card based stored value schemes. These have included both 'accounted' and 'fully distributed' schemes, all with offline capability.

Unless the target functions of a retail e-HKD are constrained, consideration of offline storage and transaction capability necessitates a technical assessment of available Trusted Execution Environments, usually relying on tamper resistant hardware.

B.5 '10 TIMES' BETTER SOLUTION TO A CURRENCY OR PAYMENT NEED OF THE TARGET USERS

Clear identification of the particular target users' currency or payment need(s) that the e-HKD could address will be critical to then designing a service, including the technical requirements, that are '10 times' better than the current alternatives that the public uses.

Any proposed central bank digital currency that is successfully adopted by the target users, involves a behavioural change by those target users.

In certain instances adoption can be mandated, particularly if the target users are regulated entities rather than the general public. However for retail CBDC, a voluntary behavioural change is the most desirable, particularly in a market such as Hong Kong where the retail payment systems are advanced, with strong competition between payment providers.

Most new retail payment systems fail to be successfully adopted, as noted by a survey of the new payment systems that emerged in the 1990s, of 200 launched only one succeeded, PayPal.

Hong Kong has at times been both a pioneer and a world-leader in new retail payment systems. For instance in the 1990s smart card-based e-cash was issued by the three note-issuing banks in Hong Kong. Unfortunately these were not 'better than cash' for small retail payments and were not successfully adopted. In contrast, the Hong Kong automatic fare collection system's (Octopus's) extension to retail payments set the global benchmark for replacement of small notes and coins by the second half of the 2000s.

The mass adoption of Octopus's retail system and other successes such as AliPay and WeChat Pay's QR based mobile payments can be attributed to being '10 times' better than the alternatives, particularly physical cash, for face to face transactions and card based payments or bank transfers for online payments.

In addition to clarification of the scope of the target market to be addressed (see above), clear identification of the particular target users' currency or payment need(s) that the e-HKD could address will be critical to then designing a service, including the technical requirements, that are '10 times' better than the current alternatives that the public uses.

B.6 TECHNICAL STANDARDISATION FOR INTEROPERABILITY WITH AT LEAST TWO PROVIDERS TO AVOID PROVIDER 'LOCK-IN' - STARTING WITH eRMB INTEROPERABILITY

Collaboration and standardisation of interfaces and critical technical components combined with competition in clearly defined areas is the 'co-opetition' model successfully adopted by major domestic, regional and global payment schemes.

At a minimum interoperability with the mainland retail CNY standard should be considered.

The paper in section 4.3 indicates a desire for the technical implementation to be flexible, interoperable and extensible.

Industry experience of payment systems and currency provide critical areas of strict standardisation and cooperation to ensure the overall risk management and robustness of the system and interoperability at critical interfaces - for example the ubiquitous interfaces between payment cards and acquiring terminal messaging as part of EMV, the standardisation of cryptographic and security minimum preventative controls etc.

At the same time there is scope for 'competition' above these areas of strict standardisation and cooperation. Within the credit card schemes this is primarily around designs, pricing and incentives. For the private bank issued notes in Hong Kong, this is only around designs, with other areas needing to meet strict standards for size and preventative security measures against counterfeit.

Comment - in order to maintain critical functional aspects of the system and interoperability, strict standardisation and cooperation will be necessary for the e-HKD CBDC technical requirements, for example strict interface API specifications, cryptographic standards etc. However, in line with the intent of section 4.3, it is recommended that the technical systems providing these capabilities should be underneath neutral interfaces, permitting at any one time at least two providers to meet the requirements. This is similar to the multiple payment terminals or payment smart card providers that compete in the market, but must all follow the same standards to ensure interoperability. There should be no component of the system that is 'locked' into a single provider.

This will inevitably constrain the desire within section 4.3 that all banks and PSPs have 'a reasonable degree of autonomy in choosing the respective technology platforms and interfaces'. The interfaces in particular should be highly standardised and participants only allowed to connect if they meet such standards (through proven testing and accreditation).

The desire to interoperate with other countries' CBDC payment systems is also referred to in section 4.3 and similarly presents challenges unless common standards are adopted. A valuable example of which would be the adoption by (China) UnionPay of a standard interoperable with EMV.

It is recommended that given the advanced state of the mainland China retail CBDC and the existing co-existence of RMB and HKD payment systems in Hong Kong, at a minimum interoperability with the mainland retail CNY standard is considered.

B.7 FIT-FOR-PURPOSE RISK MANAGEMENT APPROACH

No system is secure - each has an investment in effort to compromise a system (whether fraudulent or accidental) and losses from such a compromise need to managed in a fit-for-purpose manner.

Retail currency and payment systems generally operate on the following principles:

- Payment systems accept a manageable level of risk of losses that must be contained such that both confidence in the system and economic sustainability of the system is maintained. Credit card schemes provide an ideal example of constraining losses within an acceptable range.

- Assuming no fraudulent activity on the part of members of the system, such losses should be borne by the schemes/institutions' responsibility to protect bona fide public customers acting in good faith.

- The risk of losses is actively managed through tailored enterprise risk assessments, which in currency and payments focuses on four measures to maintain fit-for-purpose risk management:

    - prevent (usually where 'security' is applied) - detect (monitoring for abnormal behaviour) - contain (escalate or block abnormal behaviour to stem losses) and recovery (enhancement of prevent or detect controls) measures

    - constraining the 'economic' attractiveness of the target to criminal organisations, which in retail payment systems target conversion to cash or high value goods

- The balance of privacy and anonymity in currency and payment systems can be similarly addressed through a fit-for-purpose risk management approach.

    - below a certain level of value of holdings or cumulative transaction totals in a time period, the risk of anonymous or pseudo-anonymity of retail currency and payment systems is low and manageable, for example the current anonymous Octopus cards with their low fit-for-purpose limits.

    - above a certain level of value of holdings or cumulative transaction totals in a time period, the current FATF/AML rules do not permit access to the banking system without proof of identity, source of funds etc.

A fit-for-purpose risk management approach to the requirements around 'security' and 'privacy' outlined in the paper will assist in refining and assessing the technical approaches. In particular avoiding what appear to be binary assertions such as 'secure' within section 4.1 Safety, and assuming the 'highest level of standard against frauds and cyber-attacks', as the 'highest levels' should only apply to the 'highest vulnerabilities in the system and not to the lower vulnerability parts of the system. The references to 'defence-in-depth' and 'privacy-by-design' are positive, and we believe would benefit from a 'fit-for-purpose' risk management approach.

C. ADDITIONAL & THEMATIC COMMENTS BY PROBLEM STATEMENT

PROBLEM STATEMENT 1 - PRIVACY

B4 - as noted in the thematic comment on Trusted Execution Environment have a role in protecting privacy and should be considered in the overall technical assessment.

Specifically the privacy of end users maybe be protected by the following different methods:

- Dynamic public keys or addresses for each transaction

  For the dynamic public keys, different systems have different approaches:

  - Corda supports Confidential Identities and uses a different public key for each transaction are utilised by Corda, with HSM support[3]

  - Ethereum supports BIP32[4][5] key derivation and uses another derivation path index for each transaction and therefore a new key/address.

- Decoupling of transaction signature and authorization signature.

  This method provides more abstraction of the enduser and the asset. The enduser has an “approval key”, which can be used to authorize/sign transactions with the actual asset key. For example with the support of a compatible HSM, the authorizer is visible in the protected audit log of the HSM, but invisible in the actual transaction committed to the public blockchain.

B8 - as noted in the thematic comment on ‘fit-for-purpose risk management’ the application of this approach to privacy would appear to be beneficial as there is a technical need to ensure under certain circumstances such as high-value or high-risk transactions that the right to privacy is, with permission, not maintained.

Below a certain level of value of holdings or cumulative transaction totals in a time period, the risk of anonymous or pseudo-anonymity of retail currency and payment systems is low and manageable, for example the current anonymous Octopus cards with their low fit-for-purpose limits.

Above a certain level of value of holdings or cumulative transaction totals in a time period, the current FATF/AML rules do not permit access to the banking system without proof of identity, source of funds etc.

---

[3] https://docs.r3.com/en/platform/corda/4.4/enterprise/cordapps/api-confidential-identity.html

[4] https://eips.ethereum.org/EIPS/eip-601#abstract

[5] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#Abstract

PROBLEM STATEMENT 2 - INTEROPERABILITY

B6 - as noted in the thematic comment on 'technical standardisation for interoperability with at least two providers to avoid provider 'lock-in' - starting with ermb interoperability' collaboration and standardisation of interfaces and critical technical components combined with competition in clearly defined areas is the 'co-opetition' model successfully adopted by major domestic, regional and global payment schemes.

The paper in section 4.3 indicates a desire for the technical implementation to be flexible, interoperable and extensible.

Industry experience of payment systems and currency provide critical areas of strict standardisation and cooperation to ensure the overall risk management and robustness of the system and interoperability at critical interfaces - for example the ubiquitous interfaces between payment cards and acquiring terminal messaging as part of EMV, the standardisation of cryptographic and security minimum preventative controls etc.

At the same time there is scope for 'competition' above these areas of strict standardisation and cooperation. Within the credit card schemes this is primarily around designs, pricing and incentives. For the private bank issued notes in Hong Kong, this is only around designs, with other areas needing to meet strict standards for size and preventative security measures against counterfeit.

Comment - in order to maintain critical functional aspects of the system and interoperability, strict standardisation and cooperation will be necessary for the e-HKD CBDC technical requirements, for example strict interface API specifications, cryptographic standards etc. However, in line with the intent of section 4.3, it is recommended that the technical systems providing these capabilities should be underneath neutral interfaces, permitting at any one time at least two providers to meet the requirements. This is similar to the multiple payment terminals or payment smart card providers that compete in the market, but must all follow the same standards to ensure interoperability. There should be no component of the system that is 'locked' into a single provider.

This will inevitably constrain the desire within section 4.3 that all banks and PSPs have 'a reasonable degree of autonomy in choosing the respective technology platforms and interfaces'. The interfaces in particular should be highly standardised and participants only allowed to connect if they meet such standards (through proven testing and accreditation).

The desire to interoperate with other countries' CBDC payment systems is also referred to in section 4.3 and similarly presents challenges unless common standards are adopted. A valuable example of which would be the adoption by (China) UnionPay of a standard interoperable with EMV.

It is recommended that given the advanced state of the mainland China retail CBDC and the existing co-existence of RMB and HKD payment systems in Hong Kong, at a minimum interoperability with the mainland retail CNY standard is considered.

B4 - as noted in the thematic comment on Trusted Execution Environment, the critical role that technology such as HSMs or smartcards or smartphone TEEs will play in scheme, requires that there is certified standardisation on critical interfaces

(as noted above) whilst allowing multiple solution providers (avoiding single supplier 'lock-in').

HSMs are one of the technical areas, along with NFC standards for smartcards/TEEs that can and have in the past led to single supplier 'lock-in'. Ensuring that HSMs can support any current or future DLT (or non-DLT) and multiple HSM providers can be incorporated in the implementation will be important areas of consideration, with options such as generated keys being exportable and management of HSM clusters which are likely to be vendor specific.

PROBLEM STATEMENT 3 - PERFORMANCE AND SCALABILITY

Performance and scalability are a central issue to maintain confidence in payment systems. The requirements are, however, critically dependent on the scope.

B1 - as noted in the thematic comment on Scope, in order to identify the appropriate technical features of a future e-HKD system, clarification of the scope of the target market to be addressed in the ranges of 'money' and payments will be essential for ensuring fit-for-purpose capabilities.

Using Octopus automatic fare collection system as an example the overriding requirement when the system was specified in the early 1990's was to ensure that for the safety of the passengers at the mass transit gates, the transaction would occur within 300 milliseconds on a scale of at least 8 million transactions a day to cover the mass adoption by the economically active population at the time. The only technology capable of meeting this requirement at the time was fully offline contactless smartcards.

As noted in the thematic comment in section B4 and incorporated in the mainland eRMB, offline capabilities are likely to be required if the scope of the e-HKD is to current cash and notes currency. This has important implications for the technical specifications and the performance of these, as the public in Hong Kong is now expecting exceedingly fast retail transactions for both offline (Octopus) and online (AliPay, PayMe for instance).

To the extent TEEs, including backend HSMs that are expected to be critical to the technical specification, ensuring these HSMs are capable of high-performance with multi-session handling and multi-threading will be a key consideration.

PROBLEM STATEMENT 4 - CYBERSECURITY

B7 - as noted in Thematic comment 'Fit-for-purpose Risk Management' no system is secure.

The focus on 'cybersecurity' (commonly associated with gaining unauthorised access to systems[6] is a critical area of concern, however appears too narrow, as this is only one of the attack vectors to which retail CBDC systems will be exposed.

[6] https://en.wikipedia.org/wiki/Cyberattack

As an example public blockchains are exposed to the 50%+ attack of controllers of more than 50% of the CPUs power working together with hostile intent (in proof of work supported consensus) or 50%+ of the stakes (in proof of stake supported consensus).

Similarly as has been observed in June 2016 after The DAO launched on Ethereum[7], an unidentified (and hence lack of full scope of functional testing) vulnerability in the immutable 'smart' contract code can present significant risks to these systems.

All of these threats, plus others should be combined in a scheme wide Fit-for-purpose Risk Management approach to which the technical specifications will need to support and enable across the prevent, detect, contain and recover capabilities.

As noted in B7, payment systems accept a manageable level of risk of losses that must be contained such that both confidence in the system and economic sustainability of the system is maintained. Credit card schemes provide an ideal example of constraining losses within an acceptable range.

Assuming no fraudulent activity on the part of members of the system, such losses should be borne by the schemes/institutions' responsibility to protect bona fide public customers acting in good faith.

The risk of losses is actively managed through tailored enterprise risk assessments, which in currency and payments focuses on four measures to maintain fit-for-purpose risk management:

- prevent (usually where 'security' is applied) - detect (monitoring for abnormal behaviour) - contain (escalate or block abnormal behaviour to stem losses) and recovery (enhancement of prevent or detect controls) measures

- constraining the 'economic' attractiveness of the target to criminal organisations, which in retail payment systems target conversion to cash or high value goods

A fit-for-purpose risk management approach to the requirements around 'security' and 'privacy' outlined in the paper will assist in refining and assessing the technical approaches.

In particular avoiding what appear to be binary assertions such as 'secure' within section 4.1 Safety, and assuming the 'highest level of standard against frauds and cyber-attacks', as the 'highest levels' should only apply to the 'highest vulnerabilities in the system and not to the lower vulnerability parts of the system.

The references to 'defence-in-depth' and 'privacy-by-design' are positive, and we believe would benefit from a 'fit-for-purpose' risk management approach.

B4 - as noted in the thematic comment on 'Trusted Execution Environments', these have a critical role protected against cyber attacks through the storage of the key asset keys/tokens are stored in certified Hardware Security Modules (HSM), which are tamper resistant.

[7] https://en.wikipedia.org/wiki/The_DAO_(organization)

The technical specifications will need to consider such aspects as the need for all the API connections to the HSM to be encrypted between the HSM provider and the HSM. The synchronisation between the HSMs in a cluster should also be encrypted. The connection with the remote management device should also be encrypted e.g. through a secure touchscreen terminal if remote access is permitted.

It is important to determine, where the control of the keys/signatures are in a system, which is then the most vulnerable point. With an additional key authorization scheme, the control can be taken offline and split to several authorisers. It is important to note that the policy enforcement point (PEP) should be within the HSM itself to be protected against cyber attacks and not outside the security boundary.

The utilisation of Trusted Execution Environments is a specialist technical area that should be included within the technical perspectives.

PROBLEM STATEMENT 5 - COMPLIANCE

B7 - as noted in the Fit-for-purpose Risk Management thematic comment, a comprehensive Enterprise Risk assessment will need to incorporate the broad range of risks, which includes Compliance risk and how the technical specifications will incorporate the prevention, detection, containment and recovery mechanisms. Careful consideration should be given to on-going changes in compliance requirements and how these be systematically and automatically incorporated, automatically tested/certified and rolled out.

B4 - as noted in the Trusted Execution Environment thematic comment, hardware security modules will have a critical role, which includes compliance:

Attributes that should be considered in the specifications include:

- Key attestation: to prove that a key is created and stored in the HSM. Additionally, the authorization policy is part of the attestation to give evidence of the control of the key. Thus eliminating the need for elaborate key ceremonies.

- Audit features: to give audit evidence about the HSM configuration including cluster information and management information.

- Independent Certifications: FIPS 140-2 Level 3, CC 4+, eIDAS

- Compliance filters such as specifying an automatic authorization tool to ensure that the asset key can never be used without the compliance filter first validating that the transaction is compliant.

PROBLEM STATEMENT 6 - OPERATIONAL ROBUSTNESS AND RESILIENCE

B1 - as noted in the thematic comment on Scope, in order to identify the appropriate technical features of a future e-HKD system, clarification of the scope of the target market to be addressed in the ranges of 'money' and payments will be essential for ensuring fit-for-purpose capabilities.

Using Octopus automatic fare collection system as an example the overriding requirement when the system was specified in the early 1990's was to ensure that for the safety of the passengers at the mass transit gates, the transaction would occur within 300 milliseconds on a scale of at least 8 million transactions a day to cover the mass adoption by the economically active population at the time. The only technology capable of meeting this requirement at the time was fully offline contactless smartcards.

As noted in the thematic comment in section B4 and incorporated in the mainland eRMB, offline capabilities are likely to be required if the scope of the e-HKD is to current cash and notes currency. This has important implications for the technical specifications and the performance of these, as the public in Hong Kong is now expecting exceedingly fast retail transactions for both offline (Octopus) and online (AliPay, PayMe for instance).

To the extent TEEs, including backend HSMs that are expected to be critical to the technical specification, ensuring these HSMs are capable of high-performance with multi-session handling and multi-threading will be a key consideration.

B6 - as noted in the thematic comment on Technical Standardisation for interoperability, a key aspect is to avoid provider 'lock-in'.

Expanding on this principle, this implies that there is no single point of failure in the system, with sufficient redundancy and resilience specified within the technical specifications. This is an extension of the assessment of the full range of risks that a payment scheme faces and allows for horizontal and vertical scaling as well as duplication of key interface points with the multiple provider requirement as noted in B6.

B4 - as noted in the Trusted Execution Environment thematic comment, hardware security modules have a critical cryptographic role and can be a source of a single point of failure or limiting factor for robustness and resilience. As such the technical specification for HSMs should consider clustering with geo-redundance and load balancing, independent of the application being supported.

PROBLEM STATEMENT 7 - TECHNOLOGY-ENABLED FUNCTIONAL CAPABILITIES

Potential 'Innovative' need that e-HKD CBDC could address:

The significant advantages of a CDBC are the removal of issuing institution credit risk and the instant finality of settlement ('good funds') that a CDBC or CBDC backed transaction provides. Elements of the existing currency and payment systems provide these capabilities (cash, RTGS and, depending on the specific rules, local Faster Payment Systems).

Hong Kong's current private note-issuing bank currency fully backed by USD held by the Exchange Fund is a physical version of a 'stable-coins (or rather notes)' which are the subject of demand within the virtualised 'crypto' financial system, areas of which are falling under regulatory supervision for example for professional investors in Hong Kong.

One potential 'innovative' need for e-HKD CBDC to address would be a system able to support the user needs of this community, given the regulatory 'stable-coin' arrangement already exists.

The Reserve Bank of Australia's wholesale CBDC POC [8]indicated the potential benefits of enabling 'atomic' delivery-versus-payment settlement of the drawdown, novation and repayment of, in this case a tokenised syndicated loan, providing efficiency gains and reduce operational risk by replacing highly manual and paper-based processes

There is a wide range of other potential innovations across welfare, taxation, fiscal policy etc. available to the extent that the e-HKD is 'programmable'. As the recent successful Hong Kong Government Consumption Voucher Scheme[9] for all providers a restricted purpose and for certain providers an expiry date is a successful policy instrument implemented through digital 'money'. As the Economist noted in its reporting of this pioneering scheme, 'Does perishable money present the future of fiscal stimulus?'[10]

FTAHK

31st December 2021

https://ftahk.org

admin@ftahk.org

8 https://www.rba.gov.au/media-releases/2021/mr-21-30.html

9 https://www.consumptionvoucher.gov.hk/en/

10 https://www.economist.com/finance-and-economics/2021/08/07/does-perishable-e-money-represent-the-future-of-fiscal-stimulus

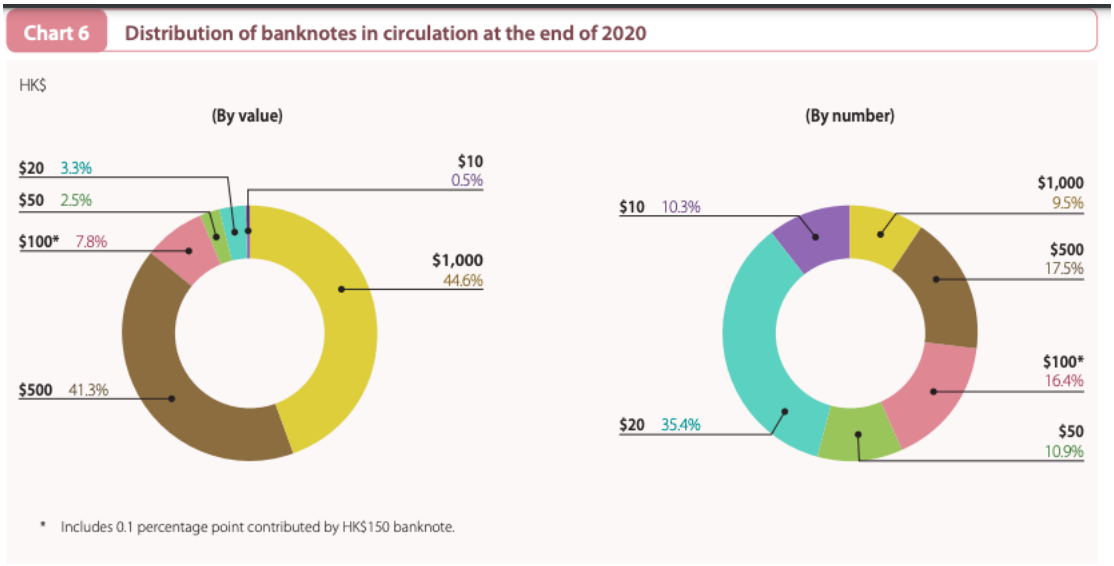
Appendix 1 - Background to Currency in Hong Kong SAR, PRC

Notes and coins issuance in Hong Kong is performed by three private note issuing banks (The Hongkong and Shanghai Banking Corporation Limited (HSBC), Standard Chartered Hong Kong Limited (SCB) and Bank of China (Hong Kong) Limited (BOC); and for the $10 and all coins by the HKMA on behalf of the Hong Kong Government.

The private bank issued notes are fully backed by USD deposited in the Exchange Fund in return for zero interest certificates of deposit (indebtedness). These are all legal tender so acceptable and fungible irrespective of the note issuing entity.

HKMA has a controlling (55%) stake in the note issuing infrastructure in the form of the Hong Kong Note Printing Limited[11]

At the end of 2020, the total value of banknotes (notes issued by note issuing banks) in circulation was HK$559.5 billion. The total value of government-issued currency notes and coins in circulation amounted to HK$12.7 billion.[12]



11 https://www.hkma.gov.hk/eng/key-functions/money/hong-kong-currency/notes/
Shareholdings: Hong Kong Government (55%) China Banknote Printing and Minting Corporation (15%) HSBC Hong Kong (10%) Standard Chartered Hong Kong (10%) Bank of China (Hong Kong) Limited (10%)

12 HKMA Annual Report 2020 - pages 65/66 https://www.hkma.gov.hk/media/eng/publication-and-research/annual-report/2020/AR2020_E.pdf

Appendix 2 - Background to the Money Supply and Retail Payment Systems in Hong Kong SAR PRC

The Money Supply in Hong Kong is subdivided as follows, with monthly analysis available from the HKMA[13], the most recent as at the end of September 2021.

	End Sep 2021
	HK$millions
Legal tender notes and coins in hands of public	564,387
Demand posits with licensed banks	1,577,334
M1	2,141,722
Savings deposits with licensed banks	3,591,439
Time deposits with licensed banks	2,298,806
Negotiable CDs issued by licensed banks and held by public	53,122
M2	8,085,088
Deposits with Restricted Licensed Banks (RLB) & Deposit Taking Co's (DTC)	12,735
Negotiable CDs issued by RLBs and DTCs and held by public	930
Total (HK$m) M3	8,098,753

Statistics are also available for money movements between banking accounts as facilitated by various payment systems in Hong Kong operated by the Hong Kong Interbank Clearing Limited (HKICL)[14].

	Sep 2021
	HK$millions
Paper Cheque Clearing	611,715
CHATS Fund Transfer	18,601,793
Faster Payment System	177,350
Electronic Clearing	5,293,829
Total HK Clearing Transaction Value (HK$m)	24,684,687

Although available less frequently, the stored value facilities (SVF's) and the card schemes also provide information on a quarterly basis.

As at the end of the second quarter of 2021, there were 64m Stored Value accounts which performed 1.5bn transactions in the quarter (1.3bn at point of sale, 0.2bn online and 0.04bn P2P) with a value of HK$62.7bn in the quarter (25.8bn at point of safe, 25.9bn online and

13 https://www.hkma.gov.hk/eng/data-publications-and-research/data-and-statistics/monthly-statistical-bulletin/

14 https://www.hkicl.com.hk/files/page_file/116/5009/2110HKD_Clg_Value.pdf

11bn P2P). The total funds held by the public in Stored Value accounts was HK$14bn at the end of September.[15]

At the end of the second quarter of 2021, there were 19.2m Credit Cards in issue, which performed 0.24bn credit payment transactions in the quarter with a value of HK$172bn. The number of debit card transactions (retail/bill payment) in the quarter was 0.04bn at a value of HK$72bn.[16]

15 https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2021/20210917e4a1.pdf

16 https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2021/20210917e5a1.pdf