December 31, 2021

Hong Kong Monetary Authority
55th Floor
Two International Finance Centre
8 Finance Street
Central
Hong Kong

Email: fintech@hkma.gov.hk

Dear Sir or Madam,

Ripple Labs Inc. ("Ripple") welcomes the opportunity to comment on the technical whitepaper on retail central bank digital currency ("rCBDC") titled "e-HKD: A technical perspective" ("the Whitepaper") published by the Hong Kong Monetary Authority ("HKMA") in collaboration with BIS Innovation Hub Hong Kong Centre ("BISIH") on October 04, 2021.[1]

Ripple also welcomes the announcement made on HKMA's new fintech strategy, Fintech 2025.[2] We strongly believe that Fintech 2025 will help leverage technology to deliver fair and efficient financial services that will benefit Hong Kong's citizens and economy. We understand that the Whitepaper forms an essential part of Fintech 2025, in order to understand the use cases, benefits, and related risks of issuing an rCBDC.

Ripple would like to thank the HKMA for both the in-depth and comprehensive analysis that has been undertaken in the Whitepaper and for the opportunity to provide our comments. We respectfully request you take them into consideration as you carefully consider the identified problem statements and key design questions. We welcome the opportunity for further correspondence with the HKMA on this Whitepaper and any other consultations as may be appropriate.

Introduction

Ripple's software products allow financial institutions to send money globally, on a real-time basis, at a fraction of the cost of traditional services available to market participants. Using blockchain technology, Ripple allows financial institutions to

---

[1] *See* https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/10/20211004-3/ Hong Kong Monetary Authority – e-HKD: A technical perspective.

[2] *See* https://www.hkma.gov.hk/eng/news-and-media/speeches/2021/06/20210608-3/, Opening remarks at HKAB Fintech Seminar: Next Phase of Hong Kong's Fintech Journey – "Fintech 2025".

process payments instantly, reliably, cost-effectively, and with end-to-end visibility anywhere in the world.

Ripple's aim is not to replace fiat currencies, but rather to enable a faster, less expensive, and more transparent method of making cross-border payments that is in the public's best interest. Ripple's customers and partners are regulated financial institutions - banks and payment service providers - who operate within the contours of the existing financial system.

Interoperability

While the Whitepaper focuses on the problem statements and key design questions related to a rCBDC, the HKMA also recognizes that a CBDC will also enable Hong Kong to take part in global initiatives that use CBDCs to improve cross-border payments. Ripple believes that interoperability - achieved through alignment of national payment protocols and adoption of international standard protocols - will ultimately be core to any successful CBDC design.

Ripple itself applies protocols to drive the efficient globalization of value through multiple initiatives with financial services and open-source communities. RippleNet, our enterprise software solution which is powered by a standardized application programming interface ("API") and built on the market-leading and open standard Interledger Protocol, enables financial institutions to facilitate faster and less costly cross-border payments. RippleNet demonstrates that deep interoperability between commercial financial institutions can make payments truly efficient, particularly in eliminating the uncertainty and risk historically involved in moving money across borders using interbank messaging alone.

In addition, Ripple offers these entities an On-Demand Liquidity capability which leverages the digital asset XRP as a bridge between fiat currencies, further reducing the friction and costs for commercial financial institutions to transact across multiple global markets. XRP is the digital asset that is native to the XRP Ledger, a distributed ledger platform.

Although Ripple utilizes XRP and the XRP Ledger in its product offerings, XRP is independent of Ripple. The XRP Ledger is decentralized, open-source, and based on cryptography. Ripple leverages XRP for use in its product suite because of XRP's suitability for cross-border payments. Key characteristics of XRP include speed, scalability, energy efficiency, and cost.

Protocols used by global, cross-border payment networks and decentralized tools that support them should be considered and supported in this new age of domestic networks, including with respect to the development of CBDCs. Embracing the capabilities of these global networks, and better enabling domestic institutions to connect their individual capabilities with other systems and markets, will enable optimized outcomes for their respective domestic needs as well as fulfill the potential that globalization of value holds.

Ripple's CBDC Private Ledger

On March 3, 2021, Ripple announced a pilot of a private version of the public, open-source XRP Ledger that provides central banks a secure, controlled and flexible solution for the issuance and management of digital currencies ("the CBDC Private Ledger").[3] The CBDC Private Ledger is based on the same blockchain technology that powers the XRP Ledger, which has supported the management of billions of dollars of value for over 8 years, without any significant security or operational issues. This also means that the CBDC Private Ledger is built for payments and designed for issuing currencies, with over 5,400 currencies issued on the XRP Ledger over the past 8 years, including XRP - which can be leveraged as a neutral bridge asset for frictionless value movement between CBDCs and other currencies.

Therefore, moving money on the CBDC Private Ledger will be cost-effective, reliable and close to instantaneous. Transactions can also happen at volumes required by central banks – the CBDC Private Ledger will handle thousands of transactions per second initially, with the potential to scale over time by using Federated Sidechains[4] or via the Interledger Protocol.

Transactions on the CBDC Private Ledger are verified by the same consensus protocol used by the XRP Ledger, which is far less energy intensive, and therefore less expensive and more efficient than public blockchains that leverage proof-of-work.[5] In fact, the XRP Ledger is a carbon neutral blockchain solution; a point of significance given the high transaction volumes required of CBDCs. In addition to leveraging the XRP Ledger technology, the CBDC Private Ledger is also supported by RippleNet technologies and the Interledger suite of protocols, to enable ultra-high throughput use-cases such as micropayments.

The CBDC Private Ledger meets even the highest of security standards for central banks, with each having complete sovereignty and ability to customize based on their own unique privacy and policy requirements. While the CBDC Private Ledger has been designed on the basis of an open-source solution - the XRP Ledger - Ripple has adapted it for use so that central banks such as the HKMA can run a private network, allowing complete control over the system.

With respect to real world applications of our CBDC solution, on September 22, 2021, Ripple announced a partnership with Bhutan's central bank, the Royal Monetary Authority of Bhutan, who will use Ripple's CBDC Private Ledger solution to pilot retail, cross-border, and wholesale payment use cases for a digital Ngultrum.[6] Ripple also announced a partnership with the Republic of Palau on November 23, 2021, which will

---

[3] *See* https://ripple.com/lp/cbdc-whitepaper, Ripple Report: The Future of CBDCs.
[4] *See* https://ripple.com/insights/a-vision-for-federated-sidechains-xrp-ledger, A Vision for Federated Sidechains on the XRP Ledger for more information on Federated Sidechains.
[5] *See* https://xrpl.org/assets/pdf/xrpl-sustainability-methodology-2020.pdf, Measuring the Environmental Impact of Cryptocurrency
[6] *See* https://www.rma.org.bt/pressrelease/PRESS%20RELEASE%20CBDC.pdf, Royal Monetary Authority of Bhutan Press Release on Pilot Project on CBDC.

initially focus on developing strategies for cross-border payments and a USD-backed digital currency for Palau.[7]

***

With this overview, Ripple respectfully submits the following responses to the problem statements and key design questions set forth in the Whitepaper in the attached Appendix.

Ripple appreciates the opportunity to provide feedback on the Whitepaper as the HKMA studies these important issues, and we would encourage and support further dialogue with all stakeholders. Should you wish to discuss any of the points raised in this letter, please do not hesitate to contact Rahul Advani (Policy Director, APAC) at radvani@ripple.com.

Sincerely,

Ripple Labs Inc.

[7] *See* https://ripple.com/insights/featured/republic-of-palau-partners-with-ripple-to-develop-digital-currency-strategy/, Republic of Palau Partners with Ripple to Develop Digital Currency Strategy.

APPENDIX

Ripple respectfully submits the following responses to the problem statements and key design questions set forth in paragraph 5 and section 3 of the Whitepaper respectively.

A. Problem statements (paragraph 5, page 2 & 3)

1. Privacy

- **To study different privacy models (e.g. anonymity, pseudonymity, metadata obfuscation, and transaction confidentiality) and their applicability to the context of rCBDC and CBDC-backed e-money**
- **To propose new designs which maintain user privacy while assuring integrity of systems (i.e. free from unauthorised manipulation) and transactions (i.e. correct recording of transactions and prevention of frauds)**

Ripple believes that separation of concern is crucial to the privacy of any system. Unless a central bank has a remit or desire to see every transaction, all the information associated between participants in a retail payment should remain private. This is where messaging layers become important, in being able to share information and keep it off-ledger but at the same time allowing the participants to access the data to support processing, including for fraud and anti-money laundering ("AML") checks. This information can then be made available to the relevant authorities as needed.

Depending on configuration, the HKMA's privacy requirements can be respected if the only area the HKMA is privy to is the wholesale CBDC. If settlement occurs in real time between the rCBDC, the only concern should be the wholesale holdings of the intermediary and the settlement between the wholesale participants. This would largely mirror the current framework adopted by most countries today.

Data integrity is a critical aspect of the CBDC Private Ledger solution provided by Ripple - all participants in a transaction all operate from a single version of the truth, and there are no copies of the data, which means that tampering and manipulation are not possible without the other parties being aware. Consideration should also be made around how and what data itself is shared, and if data is being shared without any benefit to the parties involved. Using privacy preserving technology such as zero knowledge proof-based solutions may allow only the necessary or required data to be shared.

Moreover, messaging layers mitigate a central banks exposure in the event of an insolvency by a wholesale counterparty, whilst at the same time enabling the HKMA's traceability requirements.

2. **Interoperability**
    - **To research the interoperability between conventional Financial Market Infrastructures (FMIs) and emerging Distributed Ledger Technology (DLT)-based systems based on different underlying technologies (e.g. Corda, Hyperledger Fabric, and Ethereum)**
    - **To explore emerging interoperable platforms**

Ripple has been integrating enterprise blockchain solutions into conventional Financial Market Infrastructures (FMIs) and Distributed Ledger Technology (DLT)-based systems for over 8 years through our flagship RippleNet solution, and we are in active discussions with multiple central and commercial banks regarding the use and operation of our CBDC Private Ledger.

To ensure full interoperability between intermediaries involved in the distribution of an rCBDC, the Ripple CBDC Private Ledger uses a combination of software and governance. We have learned from experience creating RippleNet, an international cross border payments system, that technology alone is not enough to ensure interoperability. While technology can support interoperability, governance is required to ensure the technology is implemented correctly.

Ripple works with the central bank to create governance that requires intermediaries to follow standards for interoperability facilitated by the software and technology of the CBDC ledger. These include using standard messaging formats like ISO 20022,[8] and network service level agreements ("SLAs"). Ripple is an active participant in the ISO 20022 Standards Body, and the first member focused on Distributed Ledger Technology (DLT).[9]

Ripple is also a leader at enabling digital currency transactions for commercial banks and payment service providers around the world. This experience has led to the CBDC Private Ledger being able to interoperate with existing systems. The APIs and libraries created, and proven, with the public XRP Ledger can be exposed and made available for integrations by stakeholders.[10] While utilizing the same technology as the XRP Ledger, the CBDC Private Ledger solution provides each central bank with its own private blockchain ledger, which is permissioned by the central bank.

The CBDC Private Ledger also has the potential to integrate by using Federated Sidechains[11] or via the Interledger Protocol, allowing the HKMA to integrate with any other DLT-based platform (e.g. Corda, Hyperledger Fabric, or Ethereum). This will enable developers to implement new features such as native smart contracts that interoperate seamlessly with the CBDC Private Ledger, while also allowing the CBDC Private Ledger to maintain its existing features.

---

[8] *See* https://www.iso20022.org/about-iso-20022, About ISO 20022.
[9] *See* https://ripple.com/lp/iso-overview/, Shaping the Future of Cross-Border Payments.
[10] Further details and documentation for developing on the XRP Ledger can be found at https://xrpl.org.
[11] *See* https://ripple.com/insights/a-vision-for-federated-sidechains-xrp-ledger, A Vision for Federated Sidechains on the XRP Ledger.

The advantages of using Federated Sidechains for an rCBDC is that it will allow for development and specialization in parallel with the main CBDC Private Ledger. For example, the HKMA can run multiple Federated Sidechains, some of which may be more private while others are more open. This essentially means that each Federated sidechain would function as its own blockchain, and the CBDC could be moved seamlessly from one chain to another.

3. **Performance and scalability**
    - **To study the trade-offs between performance and other metrics (security, privacy, etc.)**
    - **To enhance the scalability of DLT and other distributed systems with respect to increasing number of users, number of validation parties and transaction volume.**

Ripple believes that with DLT-based solutions, considerations around scaling will need to be approached in a very different manner to traditional systems, and will also be impacted by the model of participation the system adopts. There are distinct advantages to a decentralised system that enable the minimisation of single points of failure. This does raise another question around bottlenecks for individual participants if they are assigned roles in the operational running of the system, and how they scale to accommodate the load.

Whilst the above assumes a sustained throughput, considerable focus needs to be applied to looking at where there are changes to the throughput requirements through seasonal or other external factors, and how these are managed to prevent disruption. This can be mitigated with modern approaches to systems scalability that can expand and contract as required.

When thinking about performance, the underlying ledger technology is also a critical factor. Will all transactions settle in real time, and if so can the ledger scale to accommodate this? Or will it be operating in a net settlement capacity? Depending on the design, solutions such as payments being cleared on sidechains or sub ledgers, or through discrete messaging layers and settled on the main chain can be implemented.

It should also be noted that there are also advantages for having a separate clearing which include:

- The ability to add additional privacy controls and limit who can see each transaction;
- Improved processing times and the ability to scale;
- The ability to optimise liquidity at the wholesale level through the application of liquidity saving mechanisms; and
- The ability to implement discrete services that facilitate new processes or capabilities that don’t require real time settlement, or that require settlement finality once a particular state or condition is met.

4. **Cybersecurity**
    - **To enumerate the attack vectors of rCBDC systems**
    - **To propose efficient solutions to withstand high-risk attacks in order to maintain reasonable cyber-resilience, service availability and transaction security**

The CBDC Private Ledger enables all the foundational requirements underpinning industry-standard cybersecurity standards, including privacy, security, availability, integrity and confidentiality.

From a security perspective, the CBDC Private Ledger is powered by the same software that powers the XRP Ledger, which has operated for more than 8 years without any compromise of the core network. This incredible level of security is enabled by the uniquely decentralized nature of the XRP Ledger architecture - a variety of independent nodes, distributed across the globe, operate common software in-tandem without any direct coordination. This decentralized operating model is inherently superior to a centralized variant because in order to compromise the network, an attacker would need to compromise the majority of nodes, whereas in the centralized model an attacker might only need to compromise the systems of a single entity.

From a privacy perspective, the CBDC Private Ledger enforces fine-grained access control to any roles allowed by the solution, including minting, distribution, redemption and any other activities necessary to manage the full lifecycle of a national digital currency. In addition, access can be restricted in an extensible fashion, for example to actors who have been authenticated with additional security factors such as a biometric and/or hardware devices.

The deployment model of the CBDC Private Ledger also enhances user privacy by allowing a tiered topology that can isolate wholesale transactions from retail, thus shielding certain transactions from certain actors.

From an availability perspective, the decentralized nature of the CBDC Private Ledger architecture ensures that if any single node were to fail or stop responding, the rest of the network nodes would provide continuity of service. In addition, node recovery is a built-in feature of the CBDC Private Ledger such that any nodes that come online after an outage will automatically sync-up to the latest ledger state, ensuring that no node loses data.

From an integrity perspective, the CBDC Private Ledger is based upon blockchain technology employing state-of-the-art digital signature and hashing technology that allows any network participant to strongly verify the authenticity and correctness of any particular ledger operation. This contrasts to traditional ledger tracking models that rely on a single relational database, for example, that might only rely on “after the fact” auditing to detect anomalies.

From a confidentiality perspective, credentials for any account on the CBDC Private Ledger can be decentralized, and only tied back to real-world identity at the behest of the central bank and/or commercial banking partners.

On top of all this, Ripple's CBDC Private Ledger is built on a fully extensible enterprise architecture that provides for pluggability of feature-set at nearly every level. From this perspective, the CBDC Private Ledger can support any type of user-authentication system, datastore, API customizations, and infrastructure hosting and deployment model, including on-premise and cloud-based deployments.

5. **Compliance**
    - **To explore computing methods to achieve regulatory compliance goals such as AML/CFT**

Ripple believes that the compliance models adopted will be dependent on the participants in the system and what the requirements are for participation. If the existing AML/CFT processes are maintained through the intermediaries issuing a rCBDC, then a lot of the existing rules can be maintained. However, there is an opportunity to consider how these processes and participation requirements can be optimised. As the costs of compliance on a payment are currently the same regardless of the value, consideration should be made as to how this can become more linear, opening up new opportunities whilst reducing costs.

Adoption of message formats that support rich data, e.g., ISO 20022, can be leveraged to ensure sufficient information is transmitted to the other participants. Ripple has first-hand experience in seeing the impact this can have on improving straight through processing, as evidenced through RippleNet.

Beyond the existing technologies, solutions that use privacy preserving technology such as zero knowledge proof-based solutions may allow only the necessary or required data to be, shared thereby improving the privacy of an rCBDC solution whilst ensuring the participants have insight into the payment and all the parties involved.

To support data sharing and to ensure single sources of the truth are available, oracles could be deployed, thereby allowing participants to help maintain critical reference data used by other participants and have this always up to date and real time. As an example, this could take the form of a 'bad actors' list where intermediaries can log details about a bad actor to advise other participants. Consideration needs to be made on how this information is verified, but it opens up the ability to crowdsource data useful for monitoring risk and compliance.

6. **Operational robustness and resilience**
    - **To study rCBDC system designs which could operate correctly across a wide range of known operational conditions (e.g. flash transaction demand)**
    - **To study rCBDC system designs which could adapt to and recover from unforeseeable adverse conditions (e.g. offline-to-offline payments in case of connectivity outage)**

Ripple believes that it is possible to have a flexible two-tiered architecture, however considerations around the design need to be factored in to ensure the overheads can be easily managed. Critical aspects of the solution design should focus on the weak

points in a distributed and decentralised system, as the system is only ever as strong as the weakest participant.

Systems should ideally be tightly coupled. The hybrid model presented in the Whitepaper appears to rely on the synchronisation of ledger copies, which could be a potential failure point. This will require some focus to ensuring this design element is not a weak point. The expectation would be that this would also increase the operational oversight required by HKMA to operate such a model.

Considerable focus also needs to be applied at examining where there are changes to the throughput requirements through seasonal or other external factors, and how these are managed to prevent disruption. The adoption of existing scaling architecture and patterns that can expand and contract as required can be used to mitigate concerns around system scalability and can also prevent unused excess capacity.

Access to technology is another significant consideration when thinking about payment systems and building trust in any alternatives to today's payment instruments. An individual's technical understanding and whether he/she suffers from any impairments that might prevent their participation in the financial system should also not be underestimated. Design considerations that think about the user experience and ensuring that it is operationally robust to prevent user error or simple mistakes from occurring should also be included.

As part of any design of an rCBDC, the issuance, management and usage of any keys associated with the solution needs to be considered, including:

- Is there is a reliance on a phone or physical device;
- What happens if the holder loses the device, how do they recover the key and any funds associated;
- Can that device operate when there is no network connection either on the originator or beneficiary or both;
- Do limits need to be in place where network connectivity is lost;
- Can the device maintain a record of the transaction so that when it reconnects it can ensure the primary ledger is updated accordingly; and
- What are the requirements for merchants to be able to receive rCBDC payments.

7. Technology-enabled functional capabilities

- **To investigate how rCBDC solutions can improve existing business applications in terms of e.g. efficiency, security, and resilience and/or bring in new functionalities, features and applications which cannot be achieved by existing means of payments**

Ripple believes that traditional systems require the central operator to be the sole party responsible for the development and coordination of new features. This could create significant constraints and limits the innovation possible. With the underlying CBDC Private Ledger enabling an efficient framework for value exchange in a secure manner with no single actor being a single point of failure, the CBDC Private Ledger provides a platform that promotes and enables innovation through the ability to move

the rCBDC onto sidechains or sub ledgers, which allows development on these ledgers to be delivered independently of the primary ledger, and without performance or scaling concerns. These sidechains and sub ledgers can run specific versions of the ledger optimised for a particular purpose, whilst leveraging the core asset that is issued on the primary ledger.

Additionally, by leveraging a single version of the truth, new applications and services can be implemented using the rCBDC that were previously difficult or not possible with traditional systems. The ability to create new sidechains and sub ledgers also enables specific programmability or smart contracts to be defined which do not impact the main chain or other sidechains. These environments can also be used to facilitate real world sandboxes, should this be desirable, or by third parties offering innovative new services that leverage the rCBDC.

A lot of the focus on innovation has come from the programmability aspects of CBDCs, enabling everything from automated tax collection at point of sale through to condition-based payments. The CBDC Private Ledger enables these innovative solutions, as well as a myriad of other use cases, and also opens up other possibilities using Decentralized Finance (“DeFi"). The introduction of DeFi is especially important, as it allows participants who were previously unable to access financial services or markets to use the rCBDC, therefore bringing with it new ways of increasing financial inclusion.

B. Key design questions (section 3.2, page 17)

1. Over-issuance prevention

- **With minimised interaction between the wholesale and retail ledgers, can a design be certain that the two levels of ledgers are always congruent?**

It is important to note that the CBDC Private Ledger can implement both wholesale and retail CBDCs on federated blockchain ledgers. This will allow for the retail ledger's validator to own a multisign account on the wholesale ledger, ensuring the two levels of ledgers are transparent and congruent.

A federator is a piece of software that connects to at least two instances of the XRPL software. By using the federator, anyone who wants to can run a sidechain to the XRP Ledger. On one side, the federator is connected to the XRP Ledger Mainnet. On the other side, it connects to one or more sidechains. The federator would be run only by parties who operate validators on at least one sidechain. Figure 1 below provides an overview of a system with a federator and sidechains.

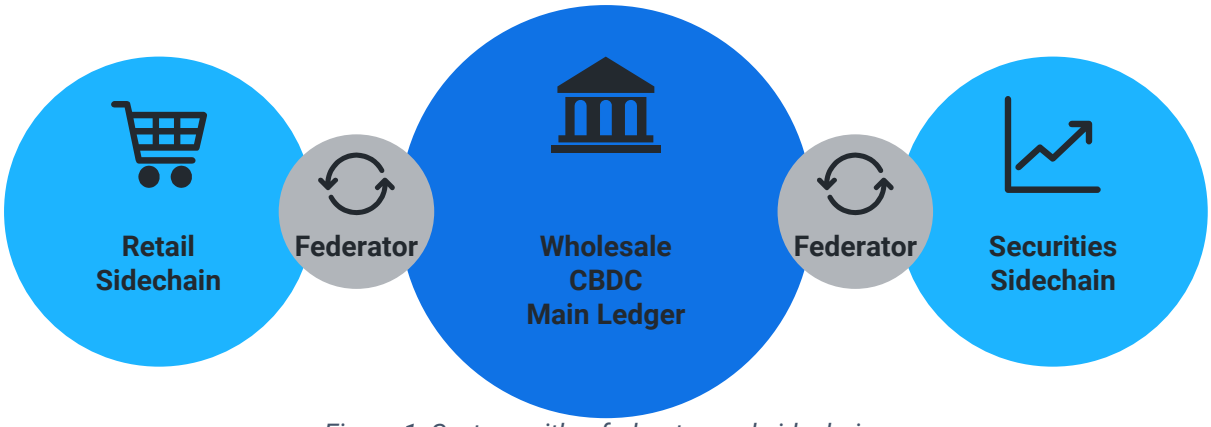

Figure 1: System with a federator and sidechains

- **Can technology help ensure that an intermediary follow the rule and protocol?**

Ripple believes that the use of DLT enables clear rules without the need for a central authority to oversee or enforce the rules. If the underlying protocol is designed and implemented correctly, this can be easily managed. The introduction of programmability can provide additional layers of enforcement. However, whilst the technology can provide technical enforcement, there will still be a need for a legal agreement that binds the obligations of the participants and ensures legal certainty when it comes to items such as settlement. Furthermore, by utilizing Federated Sidechains, the CBDC Private Ledger acts as the reference blockchain for both ledgers. This ensures that intermediaries acting on adjacent sidechains adhere to the rules and protocols set by the HKMA.

- **With intermediaries being the only channel for cross-ledger communications, can over-issuance of e-money and double spending of CBDC by an intermediary be prevented with a suitable design of transaction structure**?

Ripple believes that the underlying technology can be defined to prevent over-issuance as part of its foundation. Controls can be defined that only allow key participants, i.e., a monetary authority or central bank, from issuing a CBDC, which can be linked to underlying reserves or assets etc. When converting from a wholesale to retail CBDC, typically through a sidechain mechanism, a 1:1 relationship can be enforced which prevents over issuance. The underlying sidechain can then be used to prevent double spend. As both the wholesale and retail ledgers are blockchain solutions, they can provide complete transparency. In this way, the sidechain protocol prevents the over-issuance and double spend by intermediaries by providing a fully auditable and transparent retail blockchain ledger by the central bank.

- **Can the same structure allow detection of the traitor?**

Ripple believes that the system should be designed and implemented in a way to prevent this from being possible. By design, the CBDC Private Ledger's consensus mechanism will allow for traitors to be identified.

Validators are servers that actively contribute to the process of deciding each new ledger version. Validators only have an influence over servers configured to trust them, including indirectly. Consensus can continue even if some validators are misbehaving, including a large variety of failure cases, such as:

- Being unavailable or overloaded;
- Being partially disconnected from the network, so their messages reach only a subset of participants without delay;
- Intentionally behaving with intent to defraud others or halt the network;
- Behaving maliciously as a result of pressure from outside factors, such as threats from an oppressive government; and
- Accidentally sending confusing or malformed messages due to a bug or outdated software.

In general, consensus can continue without problems as long as only a small percentage - less than about 20% - of trusted validators are misbehaving at a given time.[12]

If more than about 20% of validators are unreachable or not behaving properly, the network fails to reach a consensus. During this time, new transactions can be tentatively processed, but new ledger versions cannot be validated, so the final outcomes of those transactions are not certain. In this situation, it would become immediately obvious that the XRP Ledger is unhealthy, prompting intervention from human participants who can decide whether to wait, or reconfigure their set of trusted validators.

The only way to confirm an invalid transaction would be to get at least 80% of trusted validators to approve of the transaction and agree on its exact outcome (invalid transactions include those spending money that has already been spent, or otherwise breaking the rules of the network).

In other words, a large majority of trusted validators would have to collude. With dozens of trusted validators run by different people and businesses in different parts of the world, this would be very difficult to achieve intentionally.[13]

2. **Privacy-preserving Transaction/Asset Traceability**
    - **Can transaction traceability be supported while preserving user privacy?**
    - **Can a design tell who is the issuer for a given amount of e-money held by a user?**
    - **Can the design tell which CBDC backing asset should be released when e-money is redeemed?**
    - **Can transactions be designed in such a way that they can provide sufficient information for the central bank to honour claims when an intermediary becomes insolvent?**

---

[12] *See* https://xrpl.org/consensus-research.html, XRP Ledger Consensus Research.
[13] *See* https://xrpl.org/consensus-protections.html#individual-validators-misbehaving, XRP Ledger Individual Validators Misbehaving.

The CBDC Private Ledger can accommodate varying levels of information traceability and anonymity. The needs and concerns of each central bank vary, and Ripple will determine the needs in solution design workshops.

Other jurisdictions have applied variable methods based on transaction and account limits. For example, a tourist might be able to purchase a card via a vending machine with a limited rCBDC balance and daily spend with just a mobile number. On the other hand, a retailer maintaining a large rCBDC balance and processing a high number of transactions would be required to onboard via a commercial bank and follow existing KYC standards.

The CBDC Private ledger is private and permissioned, allowing the central bank to grant access to desired participants. For an added layer of security, the messages accompanying a transaction can be encrypted for the desired recipient.

Additionally, an intermediated system can allow for only permissioned parties in the transaction to hold account, customer, and transaction data. In this hosted (or custodial) model an intermediary such as a commercial bank would KYC and hold the rCBDC for the end user. The end user would access the intermediary's systems to transact, and the intermediary would use their own accounts to manage the rCBDC, thus protecting the identity of the end user. Figure 2 below provides an overview of the custodial indirect distribution model.

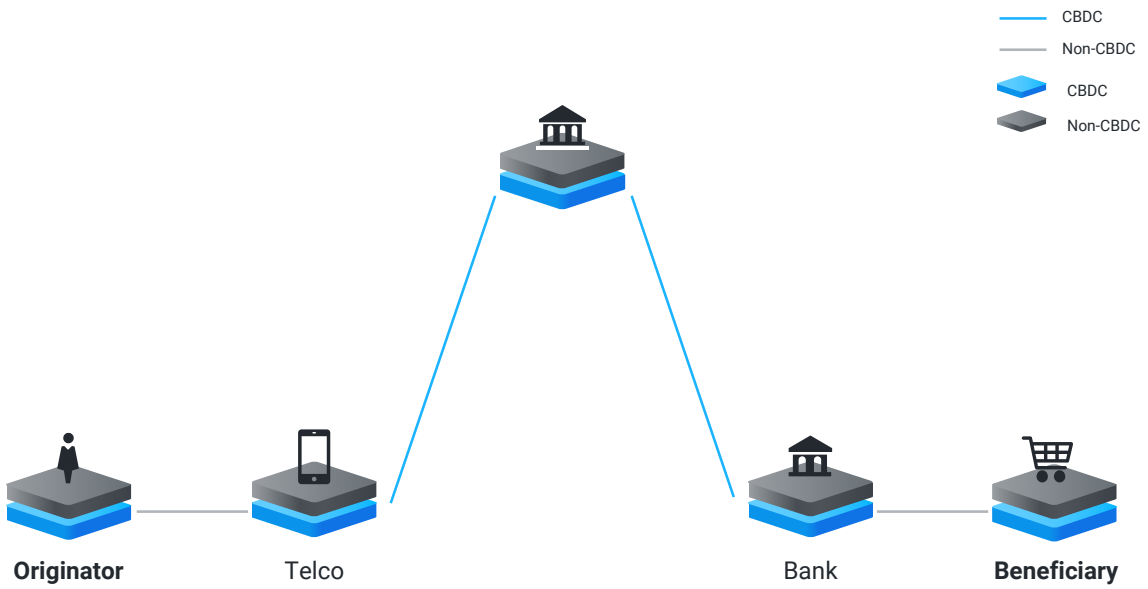

Figure 2: Custodial Indirect Distribution Model

3. **Flexible architecture**
    - **Is it possible to have a flexible architecture which can support different two-tier distribution models, including hybrid CBDC, intermediated CBDC, and CBDC-backed e-money?**

Ripple believes that it is possible to have such a flexible architecture. The functional and operational architecture of the CBDC Private Ledger enables central banks to

create flexible solutions that meet the needs of various participants. Hybrid solutions that take into account different approaches at each stage of the CBDC lifecycle can be designed. This is important as each stage of the CBDC lifecycle will have a unique set of distribution requirements, as outlined in Figure 3 below.

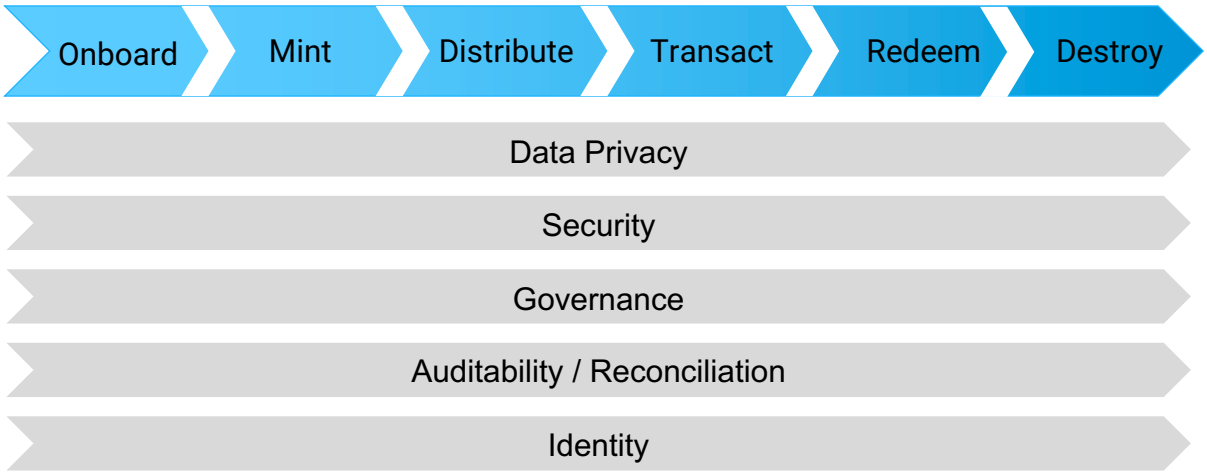

Figure 3: CBDC Lifecycle Requirements

The CBDC Private Ledger supports both an intermediated and direct approach as well as a hybrid of these methods across the lifecycle. Transactions can occur both directly between participants and/or via intermediaries, or approaches can be combined where the rCBDC is distributed through an intermediary but transactions can occur directly between participants. These models are outlined in Figure 4 (Direct Transaction), 5 (Indirect Transaction), and 6 (Hybrid Transaction) below.

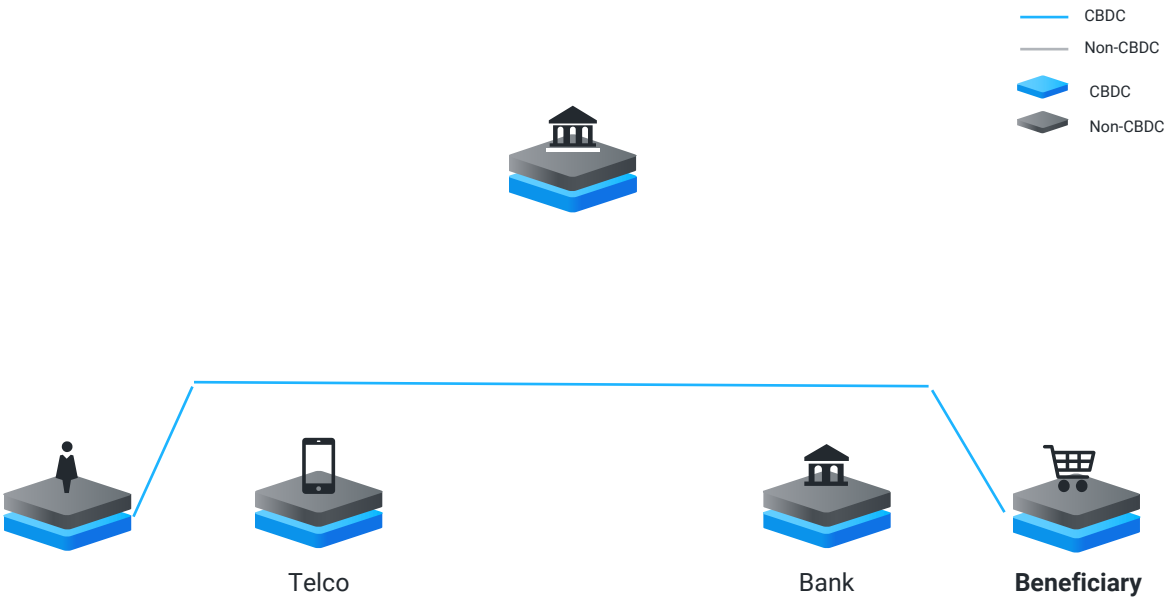

Figure 4: Direct Transaction

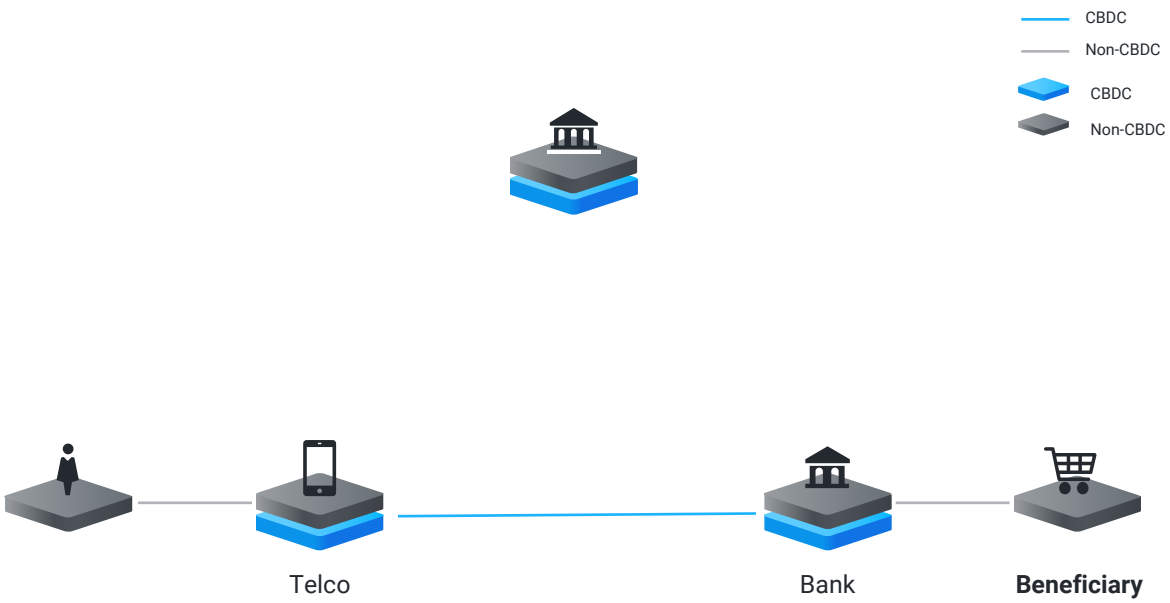

Figure 5: Indirect Transaction

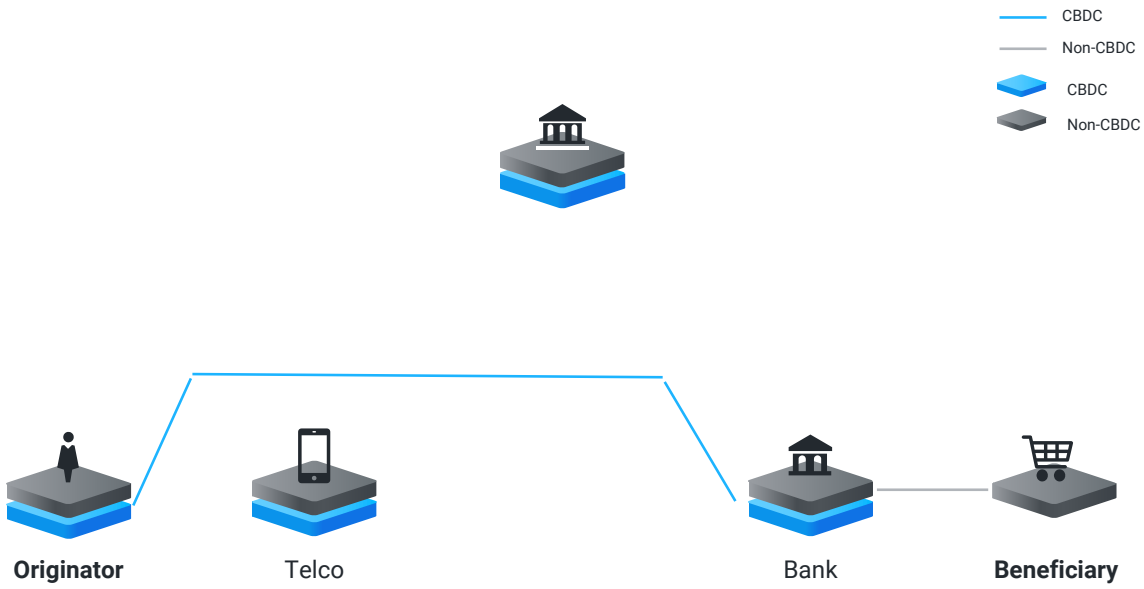

Figure 6: Hybrid Transaction

- **Can a design be modularised such that different two-tier distribution models can be instantiated through configuration of components?**

Ripple anticipates that most central banks will require a hybrid distribution approach, allowing for both direct and indirect participation in the system, and hence a design can be modularized as described.

The CBDC Private Ledger can accommodate varying levels of information traceability and anonymity. As the needs and concerns of each central bank vary, Ripple will determine the needs in solution design workshops.

- **Can the design support different types of arrangements (e.g. token vs. account) with minimal design changes?**

The CBDC Private Ledger supports aspects of both token and account systems, which obviates the needs for the unspent transaction output ("UTXO") design.

- **Can the design be extensible for new services or innovation to be built on?**

The CBDC Private Ledger is based on the public open source XRP Ledger, which has a vibrant community of developers and innovative solutions. Mobile wallets, cards, and full retail layer 2 solutions are available.

As also highlighted previously, the CBDC Private Ledger also facilitates future innovation through the use of Federated Sidechains. Federated Sidechains allow for experimentation and specialization, so that developers can enjoy the power of the XRP Ledger on a sidechain that acts as its own blockchain. For example, there is the potential to branch out into new functionality by slimming down the XRP Ledger's features to a specific subset for a particular use case, or even creating a private, parallel network for a permissioned blockchain. With Federated Sidechains, this level of extensibility is a reality.