accenture

RETAIL CBDC

Client insights and recent developments, design principles and technology considerations

CLIENT INSIGHTS AND RECENT DEVELOPMENTS

Central bank notes and coins ("cash") are in decline. Cash is incompatible with the booming digital (financial) market infrastructures. The general public relies mostly on commercial bank-issued or supported payment means to conduct digital payments. New digital private currencies are emerging offering new forms of money. Cash handling compared to digital money is expensive, risky and slow.

The future role of central banks in the retail payments space is in question. Central banks globally are discussing the best options on how to introduce a central bank digital currency (CBDC) to serve the general public, across digital platforms and channels. For example, the Swedish Riksbank is currently building a test environment to launch a blockchain based e-krona. ECB has published a report on CBDC and privacy.

CBDC could contribute to a more diversified and resilient payment system and also offer central banks an opportunity to proactively support financial innovation. It would provide instantaneous settlement, greater visibility of retail payments, allow for the introduction of interest - including the imposition of negative interest, reduce costs relative to handling cash and help prevent fraud. These features would benefit end users, merchants, intermediaries and commercial banks.

Key concerns around CBDC refer to the risk that the non-bank public may substitute bank claims for CBDC so undermining banks' business models. Also, CBDC could facilitate "bank runs" by simplifying access and storage of central bank money and thus impair financial stability. The design of CBDC would in large part determine the propensity to hold central bank money as well as transmission of monetary policy.

Bank disintermediation may occur if the public perceives important advantages to holding central bank money and banks fail to sufficiently differentiate their offerings. If CBDC is similar to bank notes, that is, constituting a non-interest bearing nominal central bank claim, CBDC holdings will likely depend on actual digital transaction and store of value needs. If CBDC were to be interest bearing, considerations to hold CBDC would also depend on savings motives and portfolio allocation objectives. Interest-bearing CBDC could significantly broaden the channel of monetary policy transmission and allow for monetary policy to have a direct impact on currency holdings, potentially increasing monetary policy effectiveness.

The approach to retail CBDC will rest on central banks' position to alter existing monetary relations between the central bank, financial intermediaries and the general public, business needs, public policy preferences and the willingness to offer a new central bank payment medium.

CBDC DESIGN PRINCIPLES

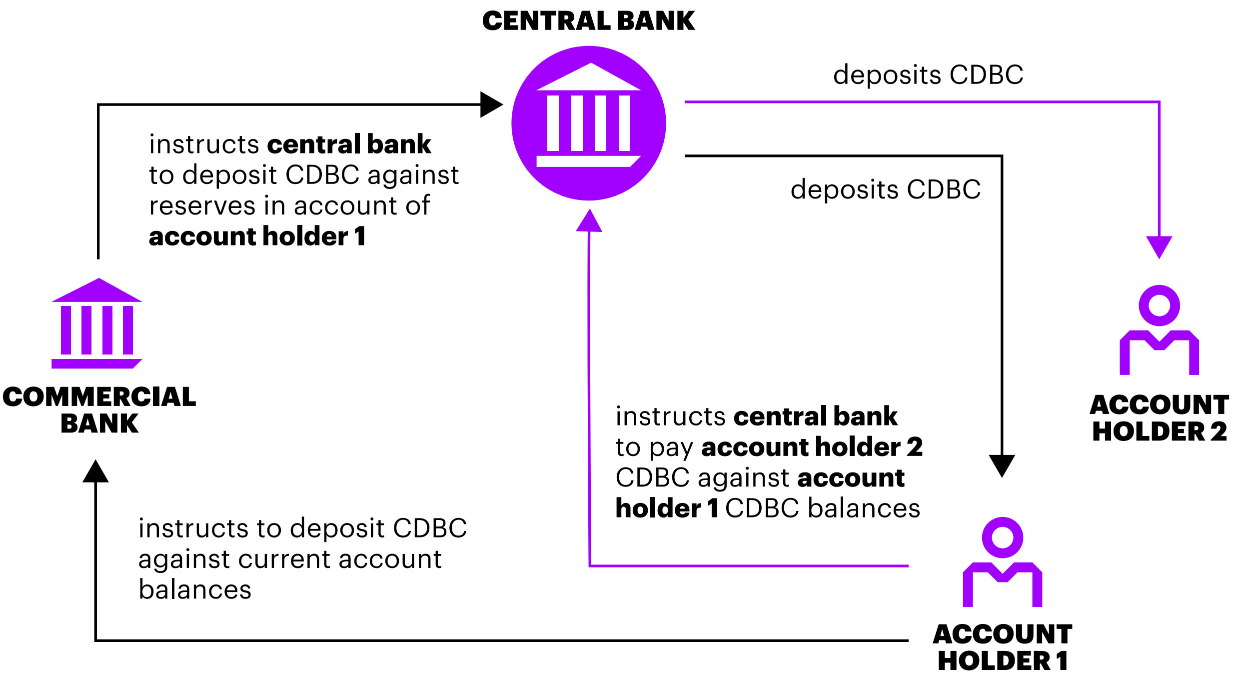
CBDC design will be driven by the specific business and functional requirements and will always entail important trade-offs. Central banks today issue cash including bank notes and often coins for the public and reserves to banks and other financial intermediaries. CBDC would constitute a third form of central bank money for the public.

Fundamental considerations for a retail CBDC rest on the selection of medium — account- versus value-based as well as the specific distribution model. An account-based approach would extend accounts at the central bank to the general public. A value or token-based approach would store CBDC locally as a digital token or bearer instrument.

In a direct distribution or one-tier approach, the central bank would distribute CBDC directly to the public. In an indirect or two-tiered approach, the central bank would distribute CBDC to commercial banks and other financial intermediaries and banks would distribute CBDC to the public.

Provisions for access to CBDC should be based on exchanging reserves for CBDC against reserves in line with existing provisions for issuing central bank money. Issuance and redemption of CBDC would constitute a simple substitution of central bank liabilities. Fungibility between CBDC, cash and reserves needs to be ensured. The distribution of CBDC in an account-based one tier approach would see the central bank issue CBDC to end-users against deposits of reserves by a financial intermediary. Financial intermediaries would thus need to remain involved to provide reserves as payment for CBDC and debit and credit the current account of the end-user (Figure 1).

FIGURE 1. ONE-TIER ACCOUNT DISTRIBUTION

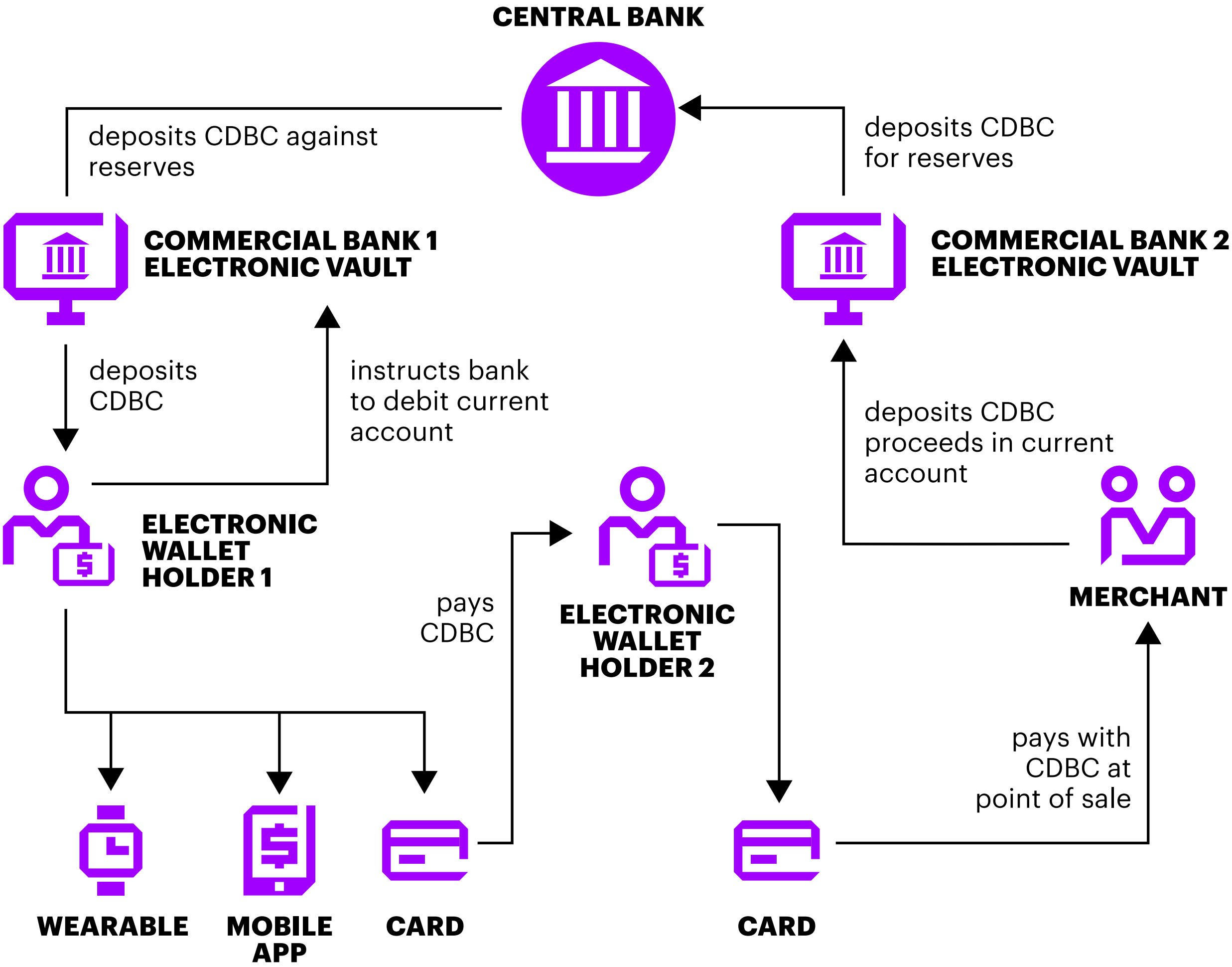


CBDC would be retired and then financial intermediaries would be credited with reserves. All transactions would be processed by the central bank similar to transactions in large value payment systems.

The distribution in a token-based two-tiered approach could rest on provisions underlying the cash cycle whereby the central bank issues CBDC against reserves to commercial banks or other financial intermediaries and commercial banks distribute CBDC to end-users against current account balances (Figure 2).

End-users can hold CBDC in different applications including but not limited to mobile phone applications, cards and wearables, e.g. watches. CBDC can be used in peer-to-peer payments and at points of sale. CBDC is withdrawn or destroyed by the central banks upon being returned by the commercial banks against crediting of reserves.

FIGURE 2. TWO-TIERED TOKEN DISTRIBUTION



CBDC TECHNOLOGY CONSIDERATIONS

The available technologies offer various architectures and provide different advantages and disadvantages in security, privacy, scalability and others. No single technology will likely meet all requirements. Technology and architecture decisions strongly depend on CBDC business design decisions.

Whether the medium is account or token-based, determines the technology platform to be used. Account-based CBDC would rely on existing account-based systems, for example, an extension of large value payment systems including real time gross settlement (RTGS) systems. The scalability of RTGS systems in terms of the number of accounts, given that accounts for the general public would entail a considerable increase in accounts, remains uncertain.

Token based systems would be based on blockchain or other distributed ledger technologies (DLT) which is considered to be the most effective to issue and manage records with features akin to a token. The token features would allow central bank money to become portable similar to a digital bearer instrument that can be transferred like sending a text. The DLT would also allow CBDC to be programmable as an embedded feature of the token.

The blockchain or DLT represents networks of independent computer-based databases (nodes) that are synchronised. The network establishes the validity of transactions on the basis of the chronological history or lineage of all previous transactions, maintaining an tamper evident record and integrity of the network. The DLT ensures a given value cannot be double spent. The DLT network offers greater resilience and security in payments as not all nodes have to be operational at all times.

DLT distinguish permissionless and permissioned networks. The former is open to the public to operate a node. The second rests on a predetermined governance structure and approval process for node operation. Only permissioned DLT networks are considered suitable for CBDC implementation. DLT technologies are evolving rapidly and any assessment of these technologies may differ in the future.

PRIVACY

The decentralized nature of DLT implies that nodes have broad (or total) visibility of transactions in the network. To restrict visibility, depending on the platform and on the application design, there is a range of mitigating techniques available, including use of pseudonyms, per-transaction pseudonyms, encryption, use of secure enclaves (such as Intel SGX), and cryptographic zero-knowledge techniques. All of these constitute a trade off against performance and scalability, cost and complexity. Not all mitigating measures are sufficiently mature.

Most of the currently available DLT technologies store all data on all nodes. Some technologies support the encryption of the data on the nodes. This ensures, as long as the encryption cannot be deciphered, that only participants with access rights (the decryption key) can read the data. Transaction contents will become visible if the private key becomes public or the encryption is compromised. The most secure way to protect data privacy, if wanted, is the physical segregation of the data and the transactions. The currently available technologies offer different solutions to ensure privacy. At the moment only very few DLT networks provide real data segregation and peer-to-peer communication between nodes.

No available DLT technology can provide real anonymity on a large scale. Real anonymity can only be provided via cryptographic methods based on zero knowledge proofs (ZKP). ZKP work in different implementations but, for the time being, more efforts are needed for an effective high volume deployment.

End-user pseudonymity can be achieved by disconnecting the real name of the end-user from used addresses. A stakeholder in the system, for example a bank, knows the connection between the real name to the address. Anonym addresses can also be issued to end customers.

Chain snipping allows the transaction history to be curtailed, thereby reducing the information present in any transaction as all transactions include the history of all previous transactions. In chain snipping tokens can be redeemed and reissued; that is the holder redeems the token with the history at the issuer and the issuer issues a new token without any history.

PERFORMANCE AND SCALABILITY

Decentralization inherently reduces performance and scalability. DLT will meet most performance requirements in payments. Residual performance deficiencies are being addressed and new approaches like sharding (network segmentation) explored.

DLT technology currently cannot support retail transactions normally performed by a user base of 100 million. Throughput depends on the DLT technology and network performance and design. Technologies are developing fast and new scaling mechanisms are under development. Technologies trying to parallelize transactions to reduce single performance bottlenecks are being explored.

INTEGRATION

A DLT based CBDC can be integrated with existing banking and payments systems using standard technologies, typically an integration layer which communicates with existing systems via APIs, message queues, or other mechanisms, as required.

INTEROPERABILITY

DLTs from different providers are normally not interoperable and require measures to establish interoperability between different DLT networks and applications. The simplest approach is integration at API level in the business application. An exchange across DLT platforms is performed through an intermediary which holds accounts in both networks (similar to accounts with correspondent banks) and the token never leaves the original network. There are mechanisms to securely synchronize transactions on two networks (for example, DvP, where delivery takes place on one network and payment on the other). Additional assurances and risk reduction may require integration at the DLT level, either by using a trusted entity that is present on both networks, or by making smart contracts on the networks aware of each other. More advanced mechanisms remain immature.

Interoperability can occur at the technological level amid a "real" transfer between two DLT networks. Transfers can take place via gateways and smart contracts. The gateway locks or destroys the token on the sender DLT network and creates the token on the receiving DLT network. The smart contract approach also uses lock/destroy and create processes in the sending and receiving DLT networks.

OFFLINE CAPABILITY

The need to conduct payment transactions when off-line require offline capabilities. Solutions exist that are similar to electronic purse systems. Mitigating measures may be needed to address residual risks in offline payments, for example, using secure applications or cards (like Geldkarte), KYC, and others including legal measures.

The development of CBDC over the next months and years is one of the most interesting topics at the intersection of public policy, business and technology.

The impact for society, the banking system and end users could be significant depending on policy and regulatory cornerstones, actual design and functionalities. Accenture will remain closely involved in the different initiatives and contribute to the speed and the scale of any positive exploration.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries — powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 509,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at www.accenture.com.

ABOUT THE AUTHORS

Dr. Nils Beier is a Managing Director in our Munich Office leading Accenture's Financial and Public Services Strategy Practice in ASGR.

John Velissarios is a Managing Director in our London Office leading Accenture's Global CBDC Practice.

Dr. Ousmene Mandeng is a Senior Advisor with Accenture's Blockchain Technology Team and co-lead of our Global CBDC Practice.

Andreas Freitag is a Senior Manager in our Vienna Office leading Blockchain and CBDC engagements.

Peter De Rooij is a Senior Principal in our London Office and Lead Architect for CBDC engagements.