Rethinking CBDC Retail Payments with Crunchfish Digital Cash Layer-2 Architecture[1]

A Practical Approach to Secure, Scalable, and Interoperable Digital Currency Transactions

The future of digital payments hinges on balancing cost, resilience, and seamless integration, bridging traditional infrastructure gaps while gearing solutions for next-generation financial landscapes. This note highlights Crunchfish Digital Cash (CDC) as a viable augmentation to a central bank digital currency (CBDC) payment system with its novel packet-switched architecture delivered by a modular and cost- effective architecture providing any underlying payment system with multiple desired design features.

Crunchfish is rethinking payments in all shapes and forms – online, offline, and even cash payments. This note briefly describes the Crunchfish Digital Cash (CDC) Layer-2 (L2) payment solution and how it augments CBDC Layer-1 (L1) systems with multiple desirable design features, such as resilience, privacy, security, scalability, interoperability, universality, seamlessness, and cost effectiveness.

Central banks are almost unanimous in their view that the ability of a CBDC to function offline is not merely a technical consideration but a key requirement. And that has spawned a growing literature on the topic from the official sector, the latest addition to which is a recently published IMF Fintech Note. However, like many other papers on offline payments, it focuses mainly on Wallet-to-Wallet considerations and gives only a light touch to the "plumbing" by which wallets interact and reconcile with online "core" ledgers. Although many vendors of offline payment solutions say that their platforms allow for indefinite operation offline, central banks are insisting that Wallets be regularly reconciled with the central ledger, to mitigate double spending risk and for financial integrity risk monitoring purposes. This note aims to rectify this omission, focusing on Crunchfish's patented CDC L2 solution.[2]

Introducing CDC: Reserve, Pay, Settle

CDC uses a Reserve, Pay and Settle approach (RPS) that assigns a value to a Wallet, reserved on the central ledger, that limits the amount a user can pay offline. To initiate an offline payment, the payer generates and transmits a cryptographically signed digital IOU ("I owe you") to the payee for an amount that accumulated, may not exceed the reserved value. The digital IOU can be validated by the payee in offline mode, and the digital credit amount may be used by the payee to make further offline payments, without synchronizing online. When either party goes online to synchronize their ledgers the digital IOUs are also validated in a Gateway before committing it on L1. This triggers a transfer of value on the central ledger from the payer's reservation to the payee.

Recently, the Bank of Canada opined favorably on the MIT Digital Currency Initiative's OpenCBDC two-phase commit (2PC) retail CBDC architecture. Like Crunchfish's RPS approach, 2PC transaction processing involves a core system update (corresponding to the RPS L1) and a wallet-to-wallet transfer (L2), with a "sentinel" checking the integrity of wallet-to-wallet transactions before core system processing. CDC L2 generalizes 2PC by also supporting offline payments. Crunchfish's RPS approach has been trialled by the Swedish Riksbank, albeit on cards only, in the fourth and last phase of the e-krona project. In general, the payment industry should be no stranger to Crunchfish's approach as it is a generalization of card payments and smart contracts.

CDC is agnostic as to whether the Wallet is implemented in a hardware secure element (HSE) or a software-based virtual secure element (VSE). The security and scalability implications of this choice was discussed in the IMF Fintech Note and summarized in Table 2. It should be noted that HSE-based solutions are challenging to scale as no ecosystem exists to deploy and upgrade a trusted payment

[1] By Joachim Samuelsson, Crunchfish CEO, with contributions from John Kiff and Chris Ostrowski.

[2] Crunchfish's foundational patent application with priority from January 2020 has been validated in 22 European countries, in the United States and Taiwan. It is patent pending in India and China. Crunchfish has also filed 14 additional patent applications on adjacent aspects, of which about half have already been granted and the others are pending being reviewed.

application across multiple mobile device models and multiple mobile network operators. This is contrasted by the easy deployment and upgrading of VSE-based trusted payment applications using standard app store ecosystems, plus the lower cost. Also, the security level for a VSE-based trusted payment application is homogeneous across mobile device models and only dependent on the isolating runtime layer provided by the integrated VSE, that mitigates double spending risks. CDC's Wallets are therefore implemented currently using a VSE security foundation.

CDC is an approved offline payment solution by the Reserve Bank of India for regulated entities since 2023 and Crunchfish is working with the National Payments Corporation of India to introduce Terminals into their payment networks. Also, Crunchfish is participating in the European Central Bank's digital euro innovation platform demonstrating three offline payment use cases with online settlement as an implementation of conditional payments, also known as smart contracts .

There are however many additional aspects that define how implementable a CBDC offline solution is in practice than just discussing the use of hardware vs. software-based secure elements. The rest of this note highlights such differences by contrasting Crunchfish's CDC with CBDC L1 systems.

Beyond Wallets: CDC as a Holistic Solution

CDC is built with Wallets, Terminals, and Gateway components with the purpose of mitigating inherent vulnerabilities in underlying L1 payment systems. It is designed to respect the roles and responsibilities of payment networks and service providers. Whereas payment service providers equip users with Wallets to initiate and make payments, payment networks need Terminals and Gateways to receive and accept payments. This clear separation of an offline payment system allows for flexibility, scalability, and healthy market competition by ecosystem participants and protects the integrity of the CBDC payment system from Wallet transactions initiated off the central ledger.

CDC allows homogeneous handling of privacy for online and offline payments managed by the banks and intermediaries. It may also be configured to incorporate anonymity and privacy thresholds. Low-value offline transactions could be allowed to be completely anonymous, whereas higher-value online and offline payments may be private up to a threshold, and beyond such threshold system traceability is required. In addition, CDC provides cross-network and cross-border interoperability, universality and seamless online and offline operation. It augments the underlying CBDC L1 system as it works across devices, regardless of proximity interaction methods.

Crunchfish's CDC ranks consistently on top when it comes to all design aspects, such as security, scalability, resilience, privacy, interoperability, universality, seamlessness, and cost. This makes it an ideal implementation companion to any CBDC L1 system. To learn more about Crunchfish and its offerings check out the homepage here, and more CDC L2 technical detail can be found here.

The Future of Payments: A Packet-Switched Architecture

CDC is based on a packet-switched architecture. This provides survivability in the face of failure on the application level, just as the internet provided resilience to digital communication. This is important to bring resilience and load balancing for online transactions. Crunchfish's signature RPS approach implemented with its CDC L2 solution allows distributed processing for offline use cases and leverages core banking systems for reconciliation. There is simply no need for an adjunct offline payment system or adjunct centralized offline payment reconciliation system for that matter. What is required is a seamlessly integrated packet-switched L2 system that respects the roles and responsibilities in the payment ecosystem.

crunchfish

IF YOU ARE A...

Payment Network Provider:

Layer-2 Terminals enable the ecosystem to receive payments.

Payment Service Provider:

Layer-2 Wallets enable the users to make payments.

Joachim Samuelsson
Crunchfish CEO

... LET'S TALK!