2024-07-29

Function Before Form: Assumptions to Avoid When Designing Retail CBDC Systems

By Joachim Samuelsson, CEO, Crunchfish

Retail CBDC systems are challenging to implement in practice. There are many features of cash that are desirable to replicate in digital form, such as the ability to pay offline and with privacy. These are rather novel features for digital payment systems as commercial payments systems tend not to offer offline payments and transactional privacy. This whitepaper highlights the problems of making premature design decisions on form without realizing its limiting consequences on the function and presents alternatives that are more suited for delivering the desired function. Defining function before form is of paramount importance for a successful implementation of CBDC in practice.

Payment system design options

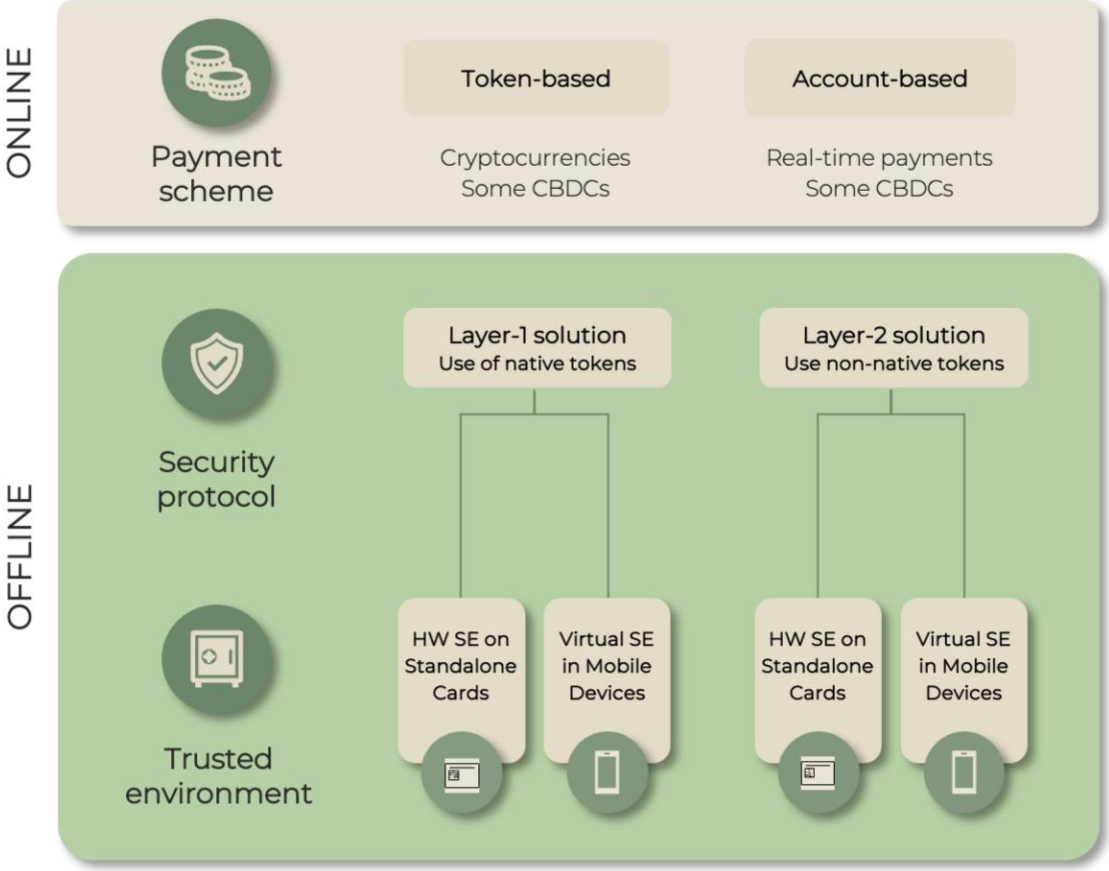

Figure 1: Payment system design options

Crunchfish in partnership with Lipis Advisors published during 2023 six whitepapers in a series Enabling Offline Payments in an Online World with the purpose of explaining how to implement offline payments in practice from multiple angles of design, security, privacy, interoperability, scalability and trust. This diagram (Figure 1) was used in each of the whitepapers to describe payment system design options from both an online and an offline perspective. It serves as an illustrative backdrop for this whitepaper also.

The first section relates to the offline security protocol. It makes the argument for a layer-2 solution where non-native digital tokens are issued offline, instead of implementing retail CBDC as a layer-1 solution using native tokens in the form of a digital banknote. The second part relates to the trusted environment on the bearer device. It outlines the many reasons why virtual secure elements are better suited for offline payments than hardware-based secure elements in mobile devices and explains why they offer better security than native software-based solutions.

Do not assume retail CBDC must be implemented as a digital banknote

Central banks issue physical cash. It is therefore understandable when imaging the form of retail CBDC that a digital banknote comes to mind. Although it is one way of implementing digital cash — the Reserve Bank of India is for instance piloting the digital rupee having fixed denominations on their digital banknotes to appear very familiar to their issued physical banknotes — it is certainly not the only way to digitalize cash.

Implementing retail CBDC as digital banknotes is technically like cryptocurrencies, albeit the central bank is the guarantee of its value. However, cryptocurrencies are only designed to work online. To avoid double-spending it is necessary to consult the online ledgers to ensure that the digital token has not been spent and to be able to transfer the exact amount to the recipient, and online exchange of tokens is necessary. As the function of offline payment is often a required function for retail CBDC it is important to be mindful when offline of not having access to the online ledgers or centrally issued token(s) that represent the exact payment amount.

Due to the above two fundamental differences between online and offline payments the function of offline payment should preferably not be implemented in the form of a digital banknote. Instead, offline payment is better implemented by the digital analogue of a banker’s cheque. The payer funds their offline wallet by requesting and paying for a banker’s cheque that can, in a trusted environment of the payer’s bearer’s instrument, be divided into smaller digital value tokens which total value may not exceed the total value of the requested banker’s cheque. These digital value tokens are issued offline at the exact payment amount to avoid issues with returning change.

A system issuing digital value tokens offline from a trusted environment in an offline wallet is an example of a layer-2 solution. It is implemented as an overlay offline payment system, often with a separate security protocol, to the underlying layer-1 online payment solution. There are many advantages of implementing offline payments as a layer-2 solution compared to implementing a layer-1 solution. A layer-2 solution offers better privacy than layer-1 solutions as there is an exchange when funding and defunding offline wallets without any traceable token trail with the offline transactions.

A layer-2 solution is also better at providing interoperability with other domestic payments schemes or other retail CBDCs. The Finternet as envisioned by BIS suggests a framework for implementing globally interoperable layer-1 ledgers. Crunchfish has suggested offline payments as globally interoperable tokens, a layer-2 solution that complements the vision of the Finternet's globally interoperable layer-1 ledgers by enabling offline transactions to other users' or merchants' cross-schemes, cross-border and cross-currencies.

Do not assume hardware-based secure elements must be used in mobile devices

A common belief is that a hardware-based secure element (SE) is always more secure than software-based virtual SE because of the clarity of security boundaries. However, due to the inevitable separation between the payment app and the hardware-based SE, there is a gap in the chain of trust between the two communicating endpoints. This can result in potential attacks by replacing either endpoint with malicious ones or tampering with them and modifying their behaviour during runtime. As the hardware-based SE does not have full visibility of the payment app and the mobile OS, it cannot determine the identity of the app or whether the app has been tampered with, and must "blindly" trust the OS and the app. A trusted client application for offline payments implemented in an app-integrated virtual secure element, on the other hand, has no trust gap issues and runs securely even on rooted/jailbroken mobile devices.

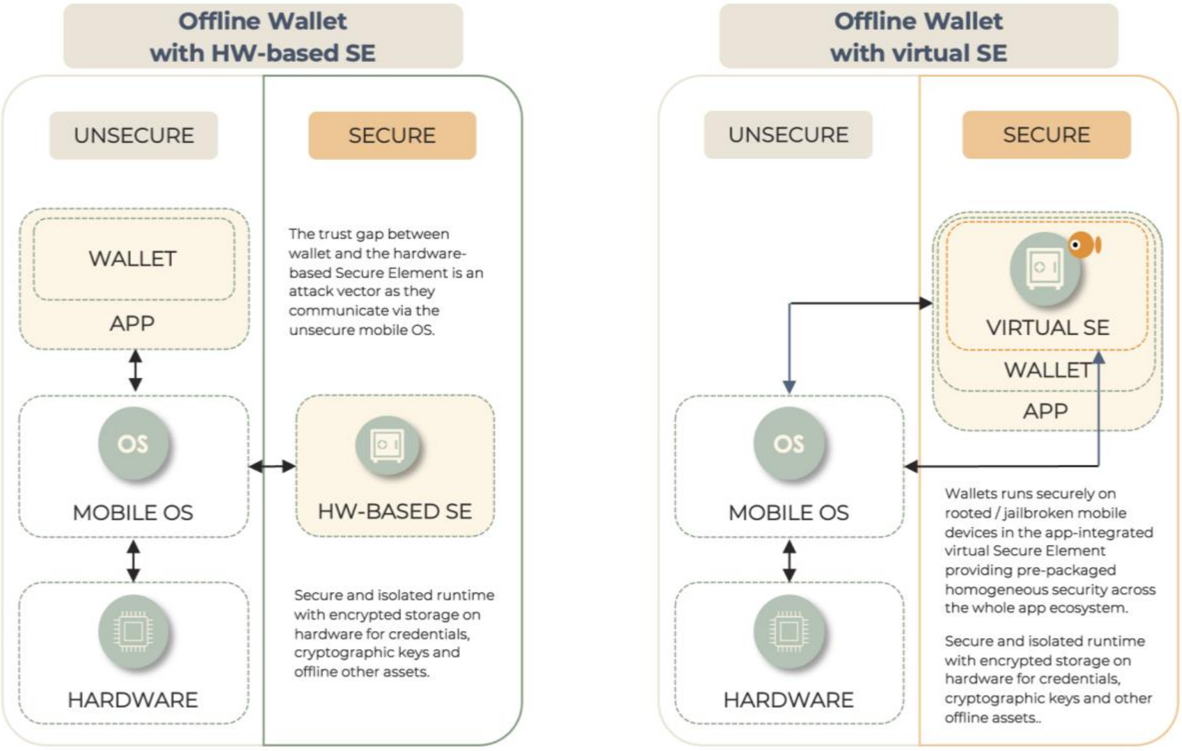
Offline Wallet with HW-based SE
UNSECURE
SECURE
WALLET
APP
OS
MOBILE OS
HARDWARE
HW-BASED SE
The trust gap between wallet and the hardware-based Secure Element is an attack vector as they communicate via the unsecure mobile OS.
Secure and isolated runtime with encrypted storage on hardware for credentials, cryptographic keys and offline other assets.
Offline Wallet with virtual SE
UNSECURE
SECURE
VIRTUAL SE
WALLET
APP
OS
MOBILE OS
HARDWARE
Wallets runs securely on rooted / jailbroken mobile devices in the app-integrated virtual Secure Element providing pre-packaged homogeneous security across the whole app ecosystem.
Secure and isolated runtime with encrypted storage on hardware for credentials, cryptographic keys and other offline assets..

Figure 2: Contrasting the unsecure architecture of a wallet using a hardware-based secure element with the secure architecture of an app-integrated trusted client application in a virtual secure element

The Handbook for Offline Payments with CBDC published by BIS in May 2023 argues that offline wallets may use hardware-based, software-based approaches or a combination of both.

> "The ability of user devices to protect data stored in purses is critical for offline payment solutions. Any solution will depend on the tamper resistance of the user device to protect against physical and cyber attacks. There are two types of approach, hardware-based and software-based, although combinations of both are common. Both hardware and software approaches offer several variations in how they implement tamper resistance. In all cases, the user device and purse combination must be designed to be tamper-resistant, because they will need to hold cryptographic keys and other data, such as the value-form and risk parameters, securely and perform cryptographic operations using those keys and data. Access to and exposure of these keys or data could result in a security breach; it is therefore critical that the hardware or software make this as hard to achieve as possible."

Even though the BIS offline handbook argues that both hardware-based and software-based solutions may be used for implementing offline payments it does not provide any insights as to why a software-based approach is a viable approach. It only refers to commercially available "white-box solutions," which are not secure enough for offline payments.

> "Software-based solutions are typically smartphone-based and use a range of software techniques to protect cryptographic keys and data both at rest and while they are being processed. Unlike hardware-based solutions, they do not require specialised components to execute their applications. Software solutions typically offer lower levels of tamper resistance than SEs or TEEs, and could use commercially available "white-box solutions" to provide tamper resistance. Software solutions would need to be separately evaluated, risk assessed and certified for assurance."

This has led many central banks to assume that they need to use hardware-based security to implement offline payments securely. This is a very unfortunate form assumption that has severe negative implications in practice and may be the foremost reason why the function of offline payments has been perceived as so difficult to implement in practice.

Software-based virtual SEs are tamper-resistant virtual machines. They offer the required security for offline payments as they provide the required isolation by a virtualized secure runtime and encrypted storage for cryptographic keys and offline assets. This is a much higher level of security than weaker software-based protection solutions that rely on a combination of code obfuscating and white-box cryptography. The primary weakness of such solutions is that the cryptography and runtime protection mechanisms run natively on unsecure hardware, which attackers can easily bypass. The key difference of using a virtual SE is that attackers cannot tamper with the offline wallet or bypass the protection mechanisms without first breaking the virtual SE itself. This is because the protection mechanisms for the virtual SE is implemented within the virtual SE, making it a secure solution.

Another key advantage of a virtual SE is that it is app-integrated. It is highly beneficial to provide the security as tightly coupled as possible with the application. It is a similar architecture to a standalone card where the hardware chip on the card is integrated with the applet. A trusted client application within a virtual SE has no trust gap issues with the payment app. This provides a consistent device-agnostic, pre-packaged level of security for the function of offline payments. It can even run securely on jailbroken or rooted devices as a compromised device does not affect the execution in the app sandbox.

The most important differences between implementing an offline payment on hardware-based or software-based virtual SEs are not related to security, but to all the other limiting factors that come with using hardware-based SEs. In addition to the burden of hardware and distribution costs, a key challenge for hardware-based solutions is that there is no ecosystem infrastructure available that supports the provision and upgrades of trusted applications on hardware-based SEs. Even if it is possible to run micro pilots on specific devices or on SIM-cards, such solutions are not scalable in practice. In contrast, device-agnostic trusted client applications in virtual SEs are built into the payment app itself and may be distributed and upgraded using the App Store for iPhones or Google Play for Android devices.

The Digital Euro project has recently published a progress report where they indicate that they are trying to address this issue. The report refers to "technical tools on the market which allow applications to be deployed remotely on the secure elements of mobile devices. These tools are commonly used for identification, telecommunications and transport purposes and could be used to deploy the offline digital euro solution too, allowing users to easily download it and use it on their mobile devices without having go to a bank branch to identify their identity."

At the same, the European Central Bank (ECB) warns that the iPhone is "incompatible with digital currency." A board member of the ECB has even written a letter to the European Commissioner for the internal market on the issue. The issue is not that the advanced iPhone is incompatible with the digital currency. Instead, it is the use of hardware-based SEs in mobile devices that is incompatible with the desired device-agnostic function of offline payments. Implementing offline payments in app-integrated trusted client applications within virtual SEs solves the problem as it is equally deployable on an iPhone as well as on any Android phone.

Hardware-based SEs in mobile devices limit the user base of the payment application to specific devices. These can be hardware-dependent by excluding devices that do not provide the required hardware-based SEs, but there is often a need to exclude users with rooted/jailbroken devices. As it is not possible to assume that all rooted/jailbroken devices can be detected, a better approach is to design an offline wallet that works securely on rooted/jailbroken devices as well. This is the case with app-integrated trusted client applications running in virtual SEs.

On a rooted/jailbroken device it must be considered that an attacker has full access to the device including the file structure of the installed apps. This means that a rollback to a previous state on the phone with a higher offline balance is an obvious attack vector. It should be noted that offline payments must protect offline data that is dynamic in nature, whereas mobile applications use only static identity data for the user and are therefore less affected by rollback attacks.

Conclusion

It is a challenge to implement retail CBDC systems as there are demands for many cash-like functions that are novel to digital payments systems. To succeed it is important to not make design decisions that limit the possibility to implement the desired function. This whitepaper has made the case for layer-2 solutions and virtual secure elements to implement cash-like features of offline payments and transactional privacy.

About Crunchfish

Crunchfish is a deep tech company developing a device-agnostic generic trusted client application platform for offline payments and tokenized card payments, as well as other mobile client/server systems. Crunchfish has been listed on Nasdaq First North Growth Market since 2016, with headquarters in Malmö, Sweden and with a subsidiary in India.

About the Author

Joachim Samuelsson has been CEO at Crunchfish AB since 2020 and a board member since 2012. Joachim is a technology pioneer and a serial entrepreneur since 1996 with successful engagements in ComOpt AB, Actix Ltd and Biomain AB. He worked at Ericsson during 1989–1996. He holds many patents in digital payments and mobile application technology and a Master of Science 1988 in Industrial Engineering and Management at Linköping University, Sweden. Born in 1965.