Offline payments and CBDC: A tale of three currencies

Eduard de Jong & Peter Cattaneo

version 1.1

Abstract

Around the globe offline payments are seen as essential for the successful deployment of Central Bank Digital Currency. Two currency technologies exist today: physical cash and bank accounts. With physical cash a payment happens between two parties; no third party is needed, it is offline. Bank accounts, on the other hand, need a third party to intermediate payments using digital technology. Any payment using an account is online and can't be offline. A third currency technology is needed to make an offline payment digitally. This third currency technology enables a two-party payment for any user at any time in any amount face-to-face and via any digital channel. This third, offline digital currency, will be essential for retail CBDC to deliver the benefits required for its practical, successful deployment and its widespread adoption by society.

Keywords: cash, e-cash, electronic cash, offline payment, account-based money.

Introduction

Central Bank Digital Currency (CBDC) is a digital form of money in that offers citizens the benefits of public money in any payment and in particular when they participate in the digital domain including in the digital economy. CBDC is a form of money that its issuer, the central bank makes available and accessible to every citizen without barriers.

A survey in The Netherlands [1] indicate that strong protection of payer privacy is a key feature that potential CBDC users want. The principle of "*privacy by design and by default*"[1] needs to be a principal consideration in choosing the technology to implement CBDC.

Another goal of CBDC is improving inclusion by giving the unbanked or underbanked access to efficient digital means of payment for bills and in shops both face to face and online. Offline payment in CBDC, untethered to a bank account, are key to achieve this goal.

Large scale adoption of CBDC could also contribute to reducing the cost of payments to society and reducing their environmental footprint.

The common approach in the design of CBDC is to focus on its **digital** nature. This led central banks to adopt the customer-account-based IT technology in use by commercial banks for its implementation. Payment with accounts is indeed digital; it is also intermediated by the operator of the database. For CBDC the central bank; in many proposals commercial banks and other parties are also involved. This resulting CBDC is an online currency.

[1] European union regulation [2] requires that the best available technology is applied in designing an IT system that processes personal data.

This paper presents an alternative for realising CBDC: electronic cash (**e-cash**). E-cash is an *offline* digital currency different from cash and from bank accounts. E-cash nicely fits the key requirements for a CBDC, privacy, convenience and inclusion.

Currency and currency technology

The technology to implement a currency is characterised by the way ownership of money is realised and the way ownership is transferred in a payment. Currency technology also addresses how money can be protected against theft and falsification and how it comes into existence.

Cash

Ownership in cash is verified possession of the objects that represent the monetary value, banknotes and coins.

The owner of the money has the task of protecting it against theft. The issuer of the money has carefully crafted the form, texture and visual aspects of each object to clearly mark them as money with explicit markings for different denominations. The money objects are manufactured under close supervision by the issuer and then *sold* to the user for their face value[2].

Payment in cash is schematically shown in Figure 1, with two user, a payer and a payee: The payer makes a payment by moving money objects from its purse to the payee. The payee upon receipt of those objects can recognise their clearly recognisable monetary value and places the objects in its own purse for safe keeping.

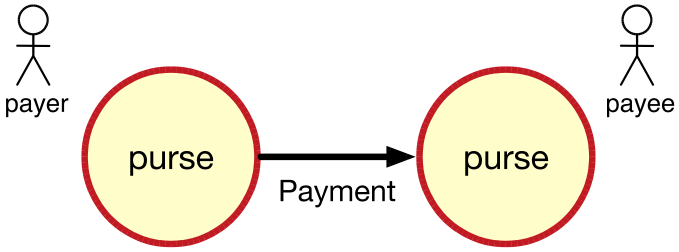

Figure 1: A cash payment involves two parties.

In a cash payment there isn't any other party present and there are no costs involved. However, in presenting the objects as money and in accepting them as payment both parties implicitly acknowledge the money issuer as the guarantor of the value of each object. The issuer is 'present' in a cash payment in a 'metaphysical' sense.

In a cash payment there is no need for either party to know any personal details related to the other party. The context of the payment fully defines the reason for the payment. In some contexts personal information may be exchanged as part of the implicit or explicit agreement that led to the payment being made.

The issuer is indirectly involved in cash payment by making money available in the form of distinct objects that each express a specific monetary value. It oversees the manufacturing of the coins and

[2] Buying a banknote for its face value binds the information encoded in the object, its denomination, directly with its inherent ability in a payment to transfer a monetary value, the face value, to a new owner. This e*ncoding theory of money* is further elaborated in [6].

banknotes and takes responsibility for the upkeep of the infrastructure to distribute these to the users. In each cash payment the issuer is passively a trusted third party.

Accounts

An account is a record in an IT system of money available to a specific user to make payments. With accounts a payment is made by changing the recorded value for both the payer and payee: the former account is reduced by the payment amount, the latter increased by it. Figure 2 shows this as a dotted arrow that starts, and ends, at the ledger where the accounts are recorded.

Figure 2 shows the additional IT infrastructure needed to make an account based payment. A bank[3] is central to making this payment. It is the entity that controls changing the account information in the ledger. The ledger is changed by the bank following a valid payment instruction from a user.

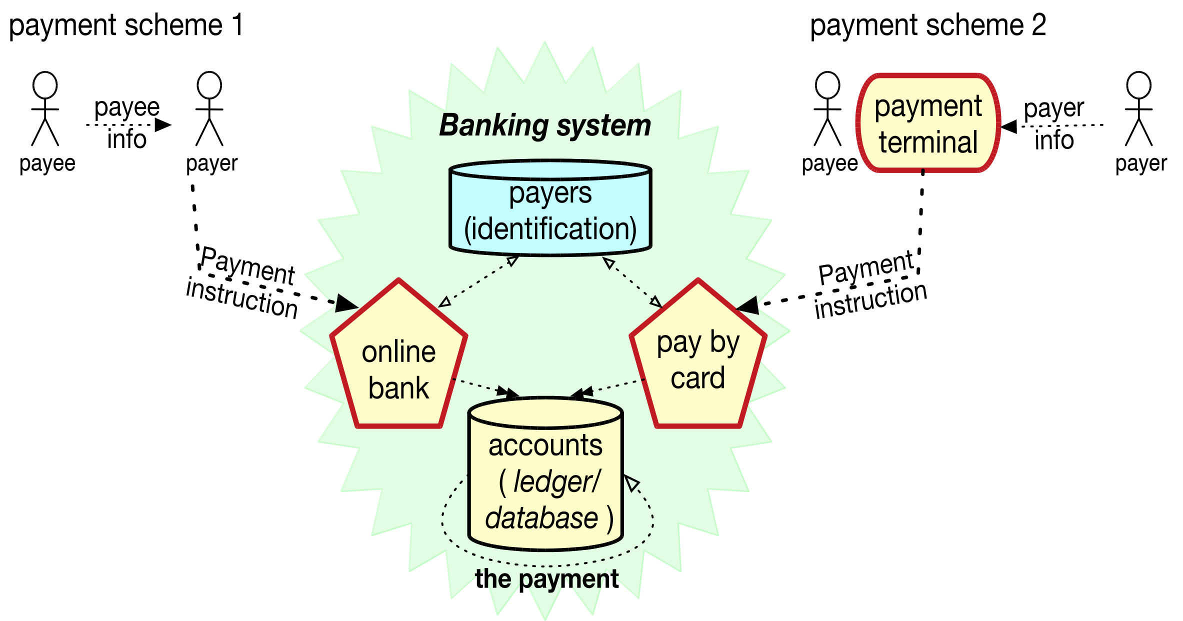

Figure 2: A bank intermediated payment involves a bank, a payer a payee and possibly other parties.

In order for a bank to recognise the instruction as coming from the payer each account is associated with payer identification data. Each payment instruction includes data that can be matched with the stored payer identification data to establish payer authorisation.

Account-based payment can support multiple 'schemes 'of payment that differ in the way the payment instruction is created or the way it reaches the bank. Figure 2 shows two of them.

In scheme 1, which could be online banking, the payer creates the payment instruction in a web page and adds information that has been obtained from the payee, e.g. the account number on an invoice, needed to make the payment to the instruction. The web page then adds the authorisation information when sending the instruction to the bank.

[3] The words “*bank”* and “*ledger*” are used in this document in a generic way and also refer to distributed ledgers, Milne [3] and Garret et al, [4] analyse that the essence of crypto currencies is a central issued money system very similar to what is shown in Figure 2 for payment scheme 1.

In scheme 2, which could be a card payment, the roles are reversed with the payee creating the payment instruction. The payee uses a payment terminal that has been configured with the required payee details to be put in every payment instruction. The payer provides his authorising personal details with a bank card, or mobile app. The payment terminal then sends the instruction to a bank for processing.

Ownership of the money in account is indirect, it is realised by the bank when it accepts a payment instruction as valid. Accepting the payment instruction is at the discretion of the bank. A reason not to accept an instruction is insufficient funds in the account, another reason could be to enforce Anti Money Laundering (AML) regulations.

Bank payments require identity information for both payer and payee to be processed in every payment. Protecting user privacy is an additional burden for the bank in addition to protecting the integrity of updates of its ledger.

Currency, currency technology and payment instruments

Comparing two figures above show that money in online digital accounts is very different from physical cash. In each of the payment systems money only flows within the system: You can transfer from account to account, or add bank notes to your wallet, but you cannot take money in your account and turn it into cash. Effectively, bank money and cash behave as if they are different currencies that requires an exchange operation to convert bank money into cash or cash into bank money. These two types of money are a different currency with the same denomination, Euros, Dollars, or Pounds. The exchange rate is 1:1.

The transfer of value between these different currencies requires either a bank teller and a vault or an ATM. In order for the bank teller or ATM to have bank notes to exchange for your digital currency, the central bank must issue additional currency and banknotes must be moved securely to the bank vault or ATM.

Kahn et al [5, page 8] describes currency technology as a “record keeping arrangement.” With bank money records are kept through accounts digitally recorded in the database. The monetary information in the records is encoded in bits and a payment changes these bits in the records for payer and payee.

Cash can also be seen as a record keeping arrangement. In this case the record is the content of the wallet held by the users. With cash monetary information is encoded by the banknotes and coins in the wallet. In a payment the information in the two records involved is updated one coin or banknote at a time.

When viewing payments as record keeping, the distinction between the arrangements in the two figures becomes irrelevant details. This is the standard economist perspective on money in a society. In this perspective every payment looks like Figure 1with the arrow defined abstractly as “*payment instrument*.[4]”

As Figure 2 shows that the payment instrument, the device that does the actual record keeping, is the bank's database. The other components in the figure support performing the 'ceremony' of the

[4] The term “payment instrument “ is further abstracted in the economist perspective as the expression of an economic actor to make a payment. This abstraction leads to recognising the *payment instruction* as a “payment instrument” a par with a bank note. It breaks down at the scale of the analysis in this paper.

payment. In contrast the instrument that changes the record in cash is the coin or banknote. The ceremony of payment with cash is handing over the coins and banknotes.

Offline digital currency technology

There exists technology[5] to make payments digitally between two parties that, just like physical cash, does not require a third party.

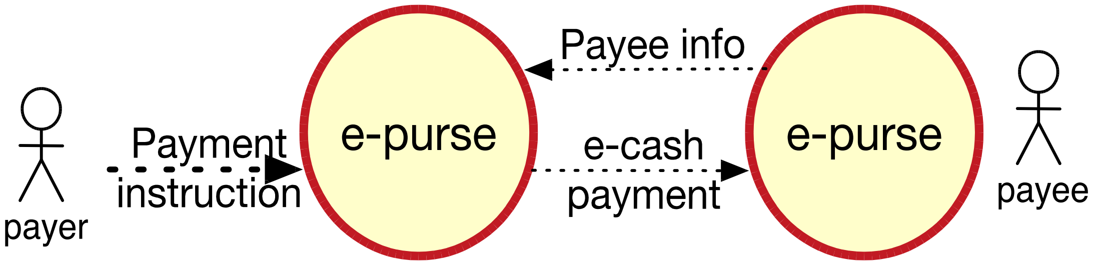

Figure 3: An e-cash payment involves two parties both equipped with an e-purse that send each other a digital message.

Such a payment is in *e-cash*. An e-purse stores money as e-cash. A payment in e-cash is finalised in the digital interaction between the two e-purses involved, involving two messages and computations in the two e-purses.

In a payment with e-cash the identity of the payer is irrelevant, it can remain hidden just like when paying with physical cash. The payee can establish beyond any doubt the validity of the e-cash received, just like with coins and banknotes.

As Figure 3 shows, a payment in e-cash is much like the payment in cash shown in Figure 1. An e-cash payment is clearly very different from a bank payment in Figure 2. As an operation with invisible digital messages, an e-cash payment requires information from the payee and an instruction from the payer to make payment to that party. This is the only similarity with a bank payment.

A payment in e-cash needs input from the payee in order to make sure the payment will be received by the correct party. The payer e-purse needs an instruction from the payer to make the payment of a specific amount to the known payee. With these inputs the payer e-purse computes the payment result. This payer computation finalises the payment and the computation result is sends to the payee e-purse to be used by the payee for further payments.

The e-purse has two sets of functions, *money* functions and *security* functions. These functions are implemented by software within the e-purses that responds to payment messages received from the other e-purse and the user instruction. The software in every e-purse is the same.

The money functions of an e-purse are: i) to store an amount of e-cash that can be spent at any time; ii) to spend money in a payment; iii) to receive money and iv) to make money available for future spending.

The security functions of an e-purse are: i) to protect the stored money as information that persists without needing power; ii) protect the amount of money against alteration except when performing

[5] A suitable e-cash technology is based on aggregating receipt token technology (ARTT). An overview can be found in de Jong [6] and a roadmap of how to build such a system in de Jong [7].

a payment; iii) perform a payment only on a valid instruction from the owner; iv) compute the data to be stored and to sent as e-cash payment based on valid payee info; v) persistently store the results of the payment computation; vi) send the e-cash payment data to the payee e-purse; vii) receive and validate the e-cash received; and viii) persistently store the money so it can used in the future.

While paying with physical cash, the money and security function are practically inseparable; in digital form each of these functions needs to be implemented explicitly. The implementation also needs to be faultless, without bugs and protected against external influences. In particular it has to be protected against an attacker intent on stealing money or on disrupting the payment system.

To meet functional and security requirements an e-purse consists of two components. A software module that can be installed on mobile phones, tablets, laptops, back office computers or cloud servers is complemented by a specially constructed secure computer, the *e-vault*, to execute the payment and security functions. The e-vault[6] is the device that keeps the money record, it is the e-cash *payment instrument*.

With e-cash the issuer is also the invisible trusted third party; it is the guarantor of the monetary value that is digitally stored, and transmitted, as money. It can fulfil this role by providing the users with e-vaults, just like it provides banknotes. The issuer also has a role to set and enforce rules for participating institutions, to supervise the system and to respond to incidents.

The issuer also issues e-cash, distributing it as an e-cash payment to banks, post offices or social services. For a bank customer withdrawal or deposit of e-cash is a payments to, or from, their own e-purse.

Conclusion

Offline digital currency, e-cash is a third form of money complementing cash and bank money. A payer of e-cash is anonymous and can pay any amount. Run-time adjustable operational parameters can be implemented to manage the velocity of money in the e-cash system.

The payment instrument in offline payment is the e-vault that securely stores an amount of money, software and security data. In a payment the e-vault computes and validates the messages between payer and payee.

An offline CBDC can leverage existing technology and experience, but it needs a ground-up design that delivers an offline currency with privacy, low-cost offline payment finality, and strong, verifiable security. An offline digital currency can deliver a user experience that is better than physical cash, while providing the issuer and its partners the visibility and control to manage and secure the system.

E-cash is essential for the success of retail CBDC. It is required to meet the social goals of money as a public good. It lowers the operational costs of the system. It improves reliability and resilience. Most importantly, it provides everyone with a way to make private, immediate, and final payments to anyone, anytime, in any amount offline, face-to-face, or online, at a distance.

[6] The technology to built an e-vault is well understood and the components to build it are readily available. Like safes and conventional vaults installed in homes and offices an e-vault can be built with different levels of physical protection that can match the amounts of e-cash stored in it.

References

[1] Bijlsma, M.; Cruijsen van der, C.; Jonker, N. & Reijerink, J. *What triggers consumer adoption of CBDC*, De Nederlandsche Bank, 2021

[2] *General data protection regulation* (GDPR), European parliament and the council, 2016

[3] Milne, Alistair K. L. *Argument by False Analogy: The Mistaken Classification of Bitcoin as Token Money*. SSRN, 2018, https://ssrn.com/abstract=3290325 or http://dx.doi.org/10.2139/ssrn.3290325

[4] Garratt, R.; Lee, M.; Malone, B. & Martin, A. T*oken- or account-based? A digital currency can be both,* Federal reserve bank of New York, 2020, https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/

[5] Kahn, C.; Rivadeneyra, F. & Wong, T.-N. *Should the central bank issue e-money*
Federal reserve bank of StLouis, 2019, https://research.stlouisfed.org/wp/more/2019-003

[6] de Jong, E. *Cash: The once and future king*
2023 https://eduard.dejongfrz.nl/papers/latest-kingreturns.pdf.

[7] de Jong, E. *How the King returns: A digital future for cash*
2024 https://eduard.dejongfrz.nl/papers/latest-howkingreturns.pdf