Digital Public Money Infrastructure (DPMI)
UoM Law and Technology Initiative
Note No.2 September 2025: Direct ownership for public digital money

E-cash with Offline Store of Value for Digital Public Money Offline Payment

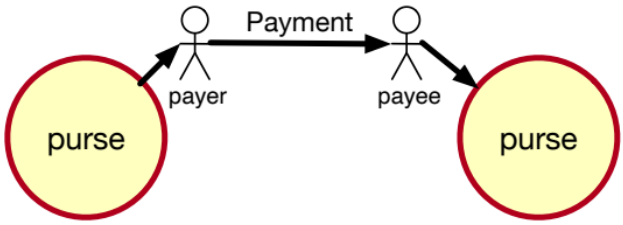
Digital Public Money, as documented in DPMI Note 1, needs electronic cash (E-cash) that is stored offline, directly available to its owner/user. This approach is significantly different from conventional digital money that is based on online access to a third party keeping user accounts. An offline store of value is essential, however, to make an offline payment, offering unique benefits of scalability, reliability, resilience, and security. This note addresses how E-cash for payments in a Digital Public Money Infrastructure (DPMI) can be realised.

An important goal of DPMI is to provide citizens and businesses full and direct access to digital payments, without dependence on foreign commercial parties and at a much lower cost. DPMI solidifies the convenience and increasing reliance on digital payments in society while also adding value through the facilitation of more direct party-to-party payments, either in person or online.

"*Direct ownership*" is what brings these enhancements to digital payments. Direct ownership means a digital payment that does not require intermediation by a bank and any other service provider, with their costs and inherent privacy protection challenges. Instead the digital information that is money is stored on a device under the exclusive control of its owner. In that device the money is ready for use in a payment; the device recognises its owner locally when instructed to make a payment.

This note uses the term "*offline digital payment"* for any payment with digital money stored in an offline device.

Figure 1



An offline digital payment is very similar to a payment in traditional cash, which is schematically shown in Figure 1. It involves a payer, a payee, and the amount of a payment moving from the payer to the payee. Yet, as we will see below in some detail, an offline digital payment is also fundamentally different: digital information is not visible and not tangible.

In a cash payment, money is handed over by the payer to the payee one coin or banknote at a time or as a stack of them. The figure shows a "*purse*" used by both payer and payee; a purse stands for any convenience device used to keep coins and banknotes together and to prevent losing money. Both parties experience their ownership of the money by seeing and handling the objects, coins and banknotes. The users are still aware of their ownership after the objects have been hidden inside a purse.

Direct ownership of digital money can't be experienced the same way as cash. A transfer of digital money is invisible and users need digital devices to learn about the result of a payment. Apart from the need for a user interface that clearly shows what is happening with digital money held offline, there are operational requirements for digital money to operate just like cash

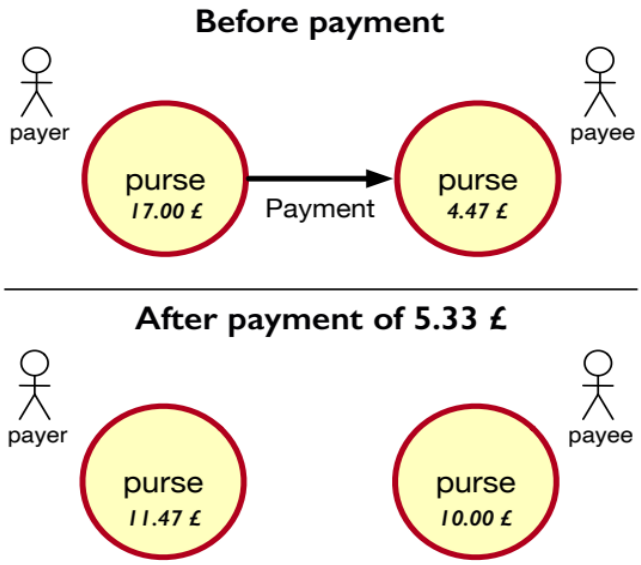
- A payment is final;
- While the payer maybe known to the payee, a payment does not require its thorough identification to be made; and
- No costs and no fees are to be paid.

Digital money with offline ownership meeting these requirements is often called "*E-cash*" (electronic cash).

Anatomy of a payment

Figure 2 illustrates a basic operational property of any payment. It shows a payer and a payee, each with a different amount of money (their balance) in their respective purses. Figure 2 is based on Figure 1 leaving out the details of handling coins and banknotes and the explicit user actions involving a physical purse that can hold these objects. With this change, Figure 2 describes any type of payment, including online and offline digital ones. With digital money, the balance is a digital number stored in a persistent memory in a computer.

Figure 2



Before the payment, the sum of the balances for payer and payee is 21.47£, after the payment that sum is still 21.47£. In a cash payment, the payment may happen in stages when each distinct money object is handed over. In each stage, the sum of balances is the same: 21.47£. In computer lingo, this fixed operational property of payments can be called the "*money invariant*.[1]"

Another operational property is that money always has an owner. The owner of cash is the owner of one of more money objects, which may be kept in a purse or wallet or in old stocking. The owner of money in a bank account is identified by the account number. In most cases, the bank-money owner is further specified by additional personal data stored in the bank database and linked to the account number. In a bank payment, that personal data is essential to recognise a payment instruction as originating from the owner.[2]

Offline digital money is stored as digital data in a specially prepared computing device that is owned and exclusively controlled by its owner. That special device - an "*E-vault*" - protects digital money, ensuring

- Effective ownership for a payer;
- The computation of an immediately final payment;
- Prevention of fraud; and
- Prevention of tampering.
-

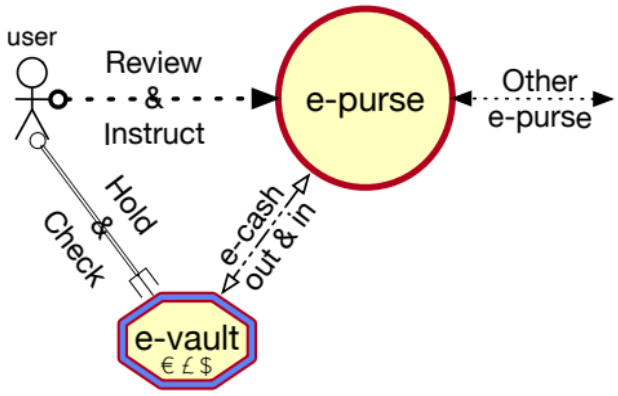
Direct ownership

Trusted computer hardware and software in the E-vault are needed to implement direct ownership. Figure 3 shows how this could be done. The E-purse is composed of software and secure hardware (the "*E-vault*"). The E-purse lets the user make a payment or review past transactions. It notifies the user of a received payment.

1 A digital system where some of the data is consistently processed while observing the money invariant meets the necessary condition for being called a money system.

2 With a crypto currency system, the money invariant is applied to the account balance data to implement a payment and the account number is a public cryptographic key. In a payment, the owner is recognised by the use of the secret counter-part of the account's public key.

Figure 3



E-purse software provides a user interface to the digital money owned by the user, handles communication with other payer or payee E-purses and communicates with the E-vault to receive or store a payment. This software runs on a user IT device with data storage and other supporting services.

The E-vault is the secure device that carries fiat currency. It is built to protect the money it holds by physical strength. *An E-vault can be built in different ways and designed at different levels of protection*. An E-vault used for everyday shopping will be built differently than the E-purse of a merchant, which will be different from the E-vault used by its supplier. Banks (including the central bank) and large corporations can store their E-cash in industry-standard Hardware Security Modules (HSM). E-vaults of any form are programmed with the same secure, cryptographically protected, offline-payment protocol. And they have all been securely initialised with the unique cryptographic secrets and certified by the central bank as fit for the purpose of storing amounts of public money.

The E-vault is programmed to securely send and receive digital money in a specific currency. It does this with a specially designed security protocol with idempotent messages, which means it is immune to interrupted communication.

The user can hold the E-vault and check it status on a display - for example,to see how much digital money it holds. The user can also store the E-vault in a strongbox; while the money in an E-vault cannot be stolen, a strongbox around it would keep it accessible to its owner. To make or receive a payment, a user does not interact directly with the E-vault. An E-purse could handle multiple E-vaults, each with the optionality of holding a different currency.

The E-purse software can be installed as an app on a mobile phone, a tablet computer, a laptop, the terminal in a point of sale (POS), or the IT system operated by a business. The E-purse software can be integrated in the administrative process, providing digitally signed proofs payment

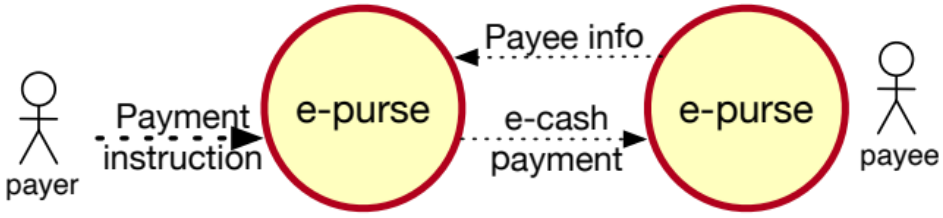
that can be entered in the administrative record, both for payer and payee. E-purse software installed on owner devices is cryptographically bound to a specific E-vault. For a user of E-cash in different denomination, an E-purse can be securely bound to multiple E-vaults.

The E-purse app may use built-in fingerprint or face matching to recognise the owner of E-cash to authorise a payment with the connected E-vault.

An E-cash payment

Figure 4 shows the information flow between in a digital payment between a payer and payee. It resembles figure x1 with a key difference: instead of objects moving from a payer to a payee, the information flows between two computers operated by the respective payer and payee.

Figure 4



As Figure 4 shows, only two E-purses are involved in an E-cash payment, one for the payee and one for the payer. No other parties are involved. It also shows, with dotted arrows, that a payment needs two messages. In the first message, the payee E-purse informs the payer E-purse where the invisible payment needs to be delivered. In the second message, labelled "*E-cash payment,*" the payer E-purse gives the payee E-purse the agreed amount of digital money.

The payer can record an E-cash payment in its digital financial administration with the E-cash-payment message combined with the unique identifying information contained in the payee-information message.[3] Unique information in this message makes E-cash resilient: in case the E-cash-payment message gets lost, the payee E-purse can resend the recorded E-cash payment.

The data in the E-cash payment is an amount of digital money on its way from payer to payee. It is money that exists outside the E-purses. Just like any other form of digital money, the E-cash payment has an owner, which clearly must be the payee. The technical form of the digital

3 Such an exchange of two-message is known in cryptography as a challenge&response protocol. As a cryptographic challenge&response the digital signature in an E-cash payment is only valid for the payment received based on specific, payment-unique payee info.

money in the E-cash payment is necessarily different from the technical form of digital money stored in the E-vault. E-cash in an E-vault is available to be spend by its owner - it is a "*spendable"* form of digital money. Defining "redemption" of E-cash as the process of adding a payment to the E-vault of its owner, the *E-cash* in the payment message is *a* "redeemable" form of digital money. Redemption of a payment can be delayed until the funds received are needed for spending.

The payer's E-vault creates the E-cash payment data after its receives the payment instruction. That instruction includes the payee info obtained from the payee. A unique identifier for the payee in this data cryptographically assures that a payment can only be redeemed with the payee's E-vault. Hence, money in an E-cash payment is owned by the payee.

The payment computation in an E-vault starts by validating a payer authorisation that has been obtained by an E-purse in composing the payment instruction. This computation maintains the money invariant by reducing the payer balance with the payment amount and immediately creating the E-cash payment. After the updated balance has been stored persistently, the E-cash payment data is send to the E-purse to be forwarded to the payee.

An E-cash payment is robust against theft, payee spoofing and communication failures. It is final by the computation in the secure confines of an E-vault. Withholding to send the result of that computation to the payee does not gain the payer. With only two parties in each payment, an E-cash system can sustain a very high number of actually simultaneous payments. A large retailer can accept simultaneous payments by deploying multiple E-purses in its POS terminals with the redeemable E-cash payments.

Conclusion

A large-scale, high-capacity, secure payment infrastructure accessible to all can be deployed through a chosen software/hardware combination in order to implement digital public money with direct ownership. In this E-cash infrastructure, a payment can be made at effectively zero costs to its users.

This implementation of digital money obeys the two system invariants that an information analysis has identified: any amount of money has an owner and the total amount of money does not change in a payment. Offline digital money meets this challenge by performing the computation of the data in an E-cash payment message, intended for the payee, in an E-vault, a secure device owned and exclusively operated by the payer. A range of cryptographic keys and algorithms are deployed on these devices under the control of the issuer for selective application based on the type of payment. In manufacturing an E-vault, the level of physical security can be

varied to match user needs, ranging from large-scale deployed citizen devices to industry standard HSMs for banks and other large corporations.

E-cash payment with immediate finality, can be securely performed in any amount and over any distance.