Digital Public Money Infrastructure (DPMI)
UoM Law and Technology Initiative
Note No.1, August 2025

OFFLINE E-CASH FOR DIGITAL PUBLIC MONEY

There is a growing requirement for Digital Public Money that is managed for the public good. Private companies have demonstrated the convenience and utility of digital money, but as society becomes increasingly digital, the limitations and risks of Private Digital Money are evident. Offline E-cash, issued and managed by a central bank, is the solution.

E-cash is digital money with offline ownership. It is a natural alternative to existing bank notes and coins that, as a digital platform, enables payments at any time and over any distance. An E-cash payment only involves the payer and the payee and is immediately final, protecting their privacy. It supports additional services from financial service providers. Managing the digital E-cash system gives the central bank, and government economists, better visibility and monetary control than with traditional cash.

Creating a 3rd Currency

The current issuance of Public Money creates two currencies: Central Bank Reserves and Solid Cash (existing bank notes and coins). The Central Bank Reserves converted to a digital format decades ago. Currencies are illustrated using the model found *here* at BIS, for comparing payment system architectures.

When e-commerce emerged, various forms of Online Private Digital Money developed to allow users to pay remotely, to pay locally without cash, and to access other benefits enabled by the digital format. Central banks looked at digital offerings in the late 1990s but didn't develop any products. After an initial period of robust development and competition, private companies shifted their focus to market consolidation and maximizing profits from a few services.

The solution is for the central bank to create a third currency, E-cash. These figures show each currency as a box using a different colour. Since they are the same denomination, they are shown as shades of blue. Each is a closed system. How they interoperate is illustrated in the following sections.

Figure 1: Two Currencies

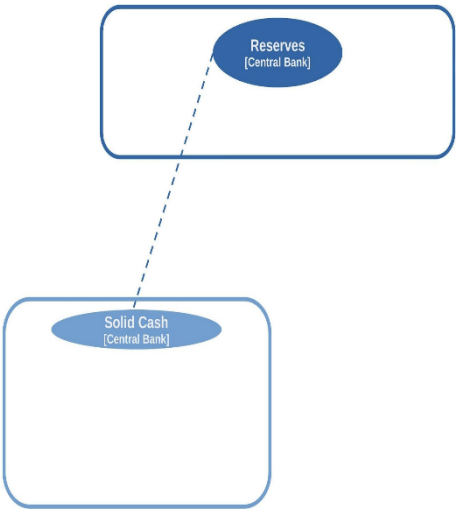
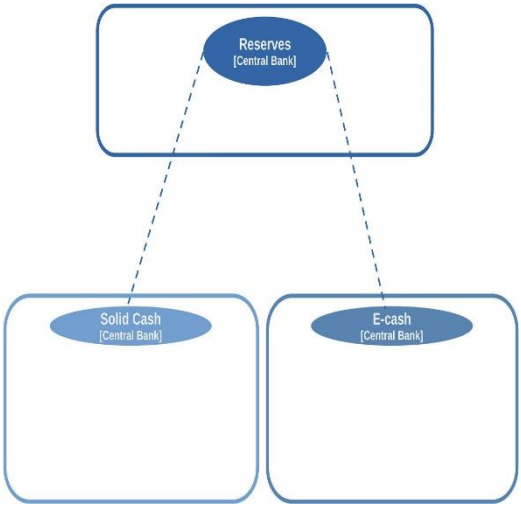


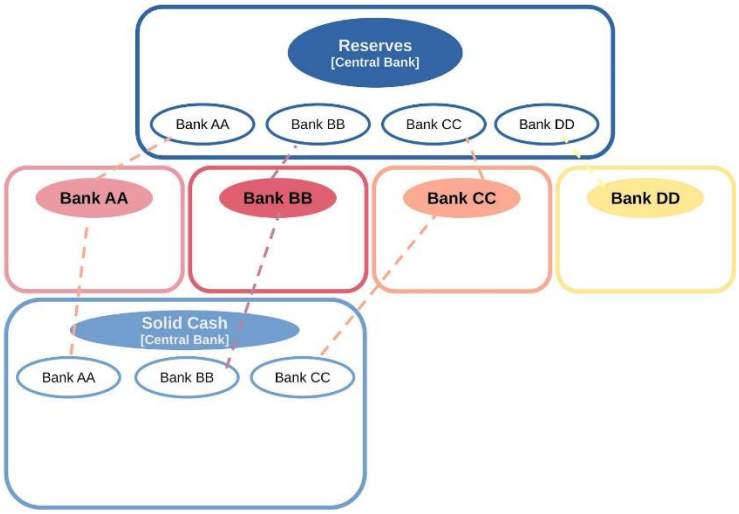
Figure 2: E-cash – a Third Currency



Working with Banks

Banks manage their own Private Money, as shown by the different colors representing the different currencies. Each bank maintains an account in the Central Bank Reserves, as shown by the blue ovals within the closed system bounded by the blue line for this currency. These accounts are linked to each bank, as shown by a dashed lines. Central Bank Reserves and Solid Cash remain linked as shown in Figure 1. The blue dotted line is not shown to focus on the other links. Banks AA, BB, and CC, maintain cash accounts as shown by the lighter blue ovals and links to the Solid Cash closed system. In Figure 3, Bank DD, does not support cash.

Figure 3: Bank Participation

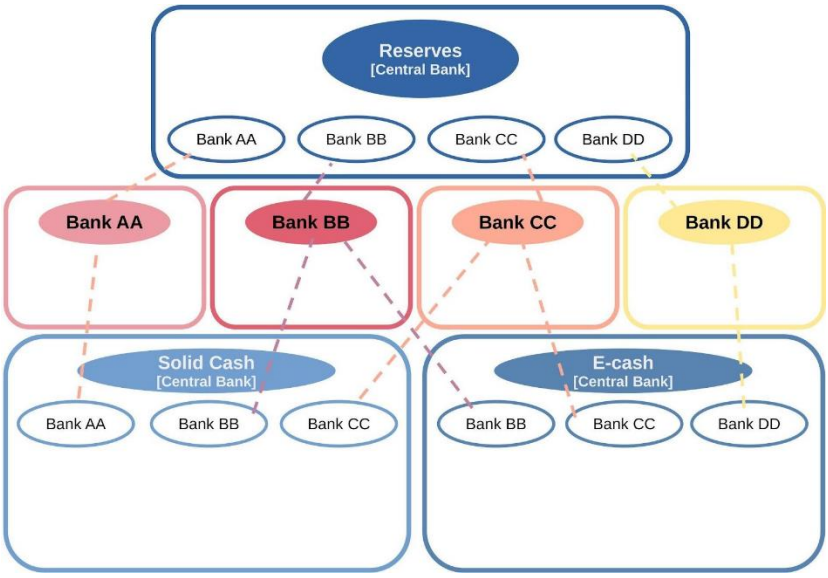


Funds for Central Bank Reserves, both at the central bank and in the accounts for the banks shown in blue inside that closed system are held on digital ledgers. Private Money at individual banks is also held on digital ledgers.

Solid Cash is physically held in vaults at the central bank and at banks participating in this closed system. Transfers within each closed system can be made directly. Ledger systems manage balances for different accounts. Within a closed system, balances can be updated in tandem. Cash systems send and receive bank notes. Transfers between systems require paired transactions. These inter-system transfers (between currencies) require liquidity for both transactions. For example, the central bank can only issue currency in the Solid Cash closed system if they have enough bank notes in their vault. When a consumer makes an ATM withdrawal, they must have an adequate balance in their account at that bank. The bank must have enough bank notes available in their ATM. In all cases, when transfers occur between different currencies, both sides must have liquidity. Money cannot simply be created and destroyed randomly. Monetary supply must be managed.

The E-cash system creates a third currency that works like Solid Cash. As shown in Figure 4, Banks BB, CC, and DD participate in the E-Cash system. The money is held offline in individual E-purses. This provides the foundation for a system with privacy, resilience, scalability, and resistance to central attack. Just as with Solid Cash, banks can engage with E-cash or not.

Figure 4: Banks and Solid Cast and E-cash

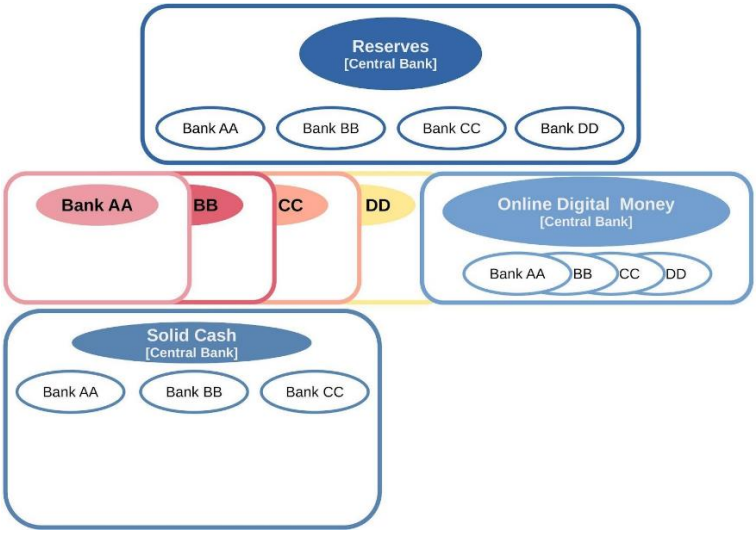


Because E-cash is digital, there are additional opportunities for value-added services that can be provided by banks or others. These services may include insurance, cross border payments, automated cash sweep, bank account linkage, and many others. As a digital system, any "smart" service can be added. Policy constraints are under the control of the central bank.

Contrast with Online Digital Money

Central Bank Online Digital Money as analysed by Bank of England, European Central Bank, Bank for International Settlement and other organizations that have focused on ledger-based digital currencies and off-the-shelf products is shown here in Figure 5.

Figure 5: Online Digital Money



In this approach, Central Bank Digital Money is like private bank digital money, with an online account for each user. It is a third currency, in addition to Central Bank Reserves and Solid Cash. It adds a closed system shown in lighter blue, with a number of User accounts.

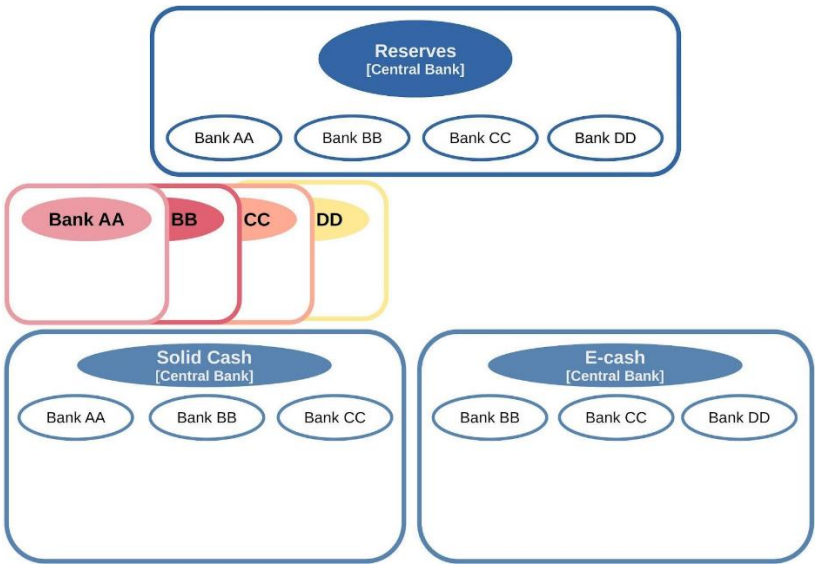
These Users can be banks, corporations, retailers, end-users… any entity that the central bank allows to create an account.

Privacy is challenging because account information is required for each payer and payee. Accounts are associated with each individual. Adding privacy requires additional levels of complexity to obfuscate identity. This creates operational cost... forever. Preventing the system operator from controlling each transaction and possibly blocking access requires additional complexity. Because the system is centralized, scaling is expensive, with real-time always-on systems required. The system has little resilience, as transactions must be routed through a central ledger. Mitigating these risks adds cost and complexity.

Online Digital Money cannot support offline payments. The money only exists in online accounts within the closed system boundary for that currency. Payment is not final until the account is updated.

In contrast, Offline Digital Money supports payments locally or remotely using any digital communication channel. The difference is in where the money is stored. Offline money can be transferred to any E-purse regardless of where it held. The E-purse receiving payment can be in the same location as the Payer or in the back office of an online retailer.

Figure 6: Offline Digital Money



Requirements analysis for Central Bank Digital Currency show that offline payment is required. E-cash is the solution. As an Offline Digital Money System that delivers a cash-like experience including both offline payment and online payment, E-cash is the one additional currency that meets all the requirements.

How E-cash works

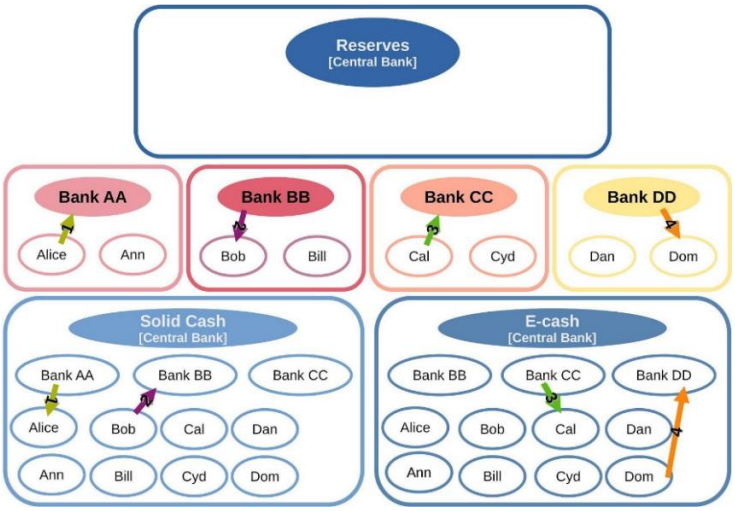
E-cash is shown in the context of banks in Figures 7, 8, and 9. As with Solid Cash, much of the distribution of this currency will be done by banks. E-cash can also be distributed through other organizations to enhance inclusion, resilience, and other important social values, as will be illustrated in the next section.

Solid Cash is a currency where value is held as bank notes and coins in wallets and vaults as shown in Figure 7. The ovals within the Solid Cash boundary and in the Solid Cash color represent these stores of value. E-cash is a different currency, with its own boundary and color. The ovals represent the digital store of value that is held in E-purses.

These E-purses provide a secure environment managed by the central bank. The use of the E-cash in the E-purse is fully under the control of its owner just like the cash in a wallet.

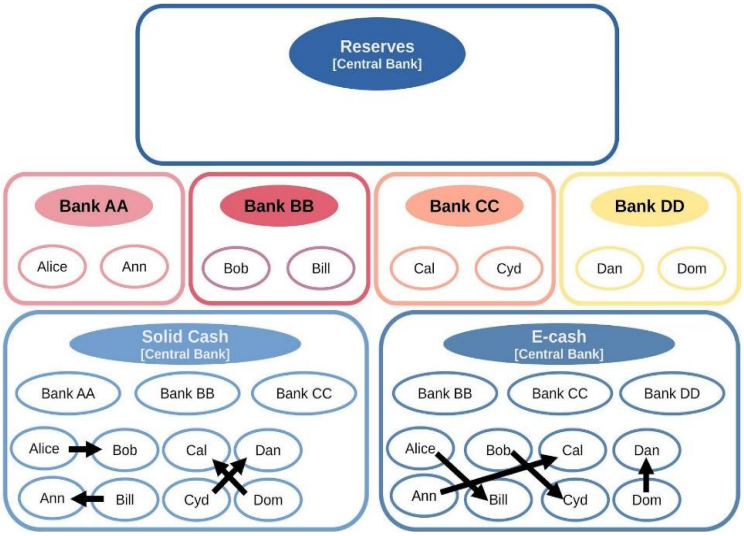
Paired transactions for withdrawing and depositing cash and E-cash are shown by the arrows in Figure 7. Arrow 1 in Bank AA shows the debit to Alice's account while the corresponding arrow 1 in Solid Cash is where the bank delivers the same amount to her in bank notes and coins. The process is exactly the same for E-cash. Cal's account at Bank DD is debited as E-cash is delivered to his E-purse. Cash deposits are illustrated by arrows 2 & 4.

Figure 7: Withdrawals and Deposits



Payments are shown in Figure 8. Because these payments are between offline stores of value, these payments can happen simultaneously without putting any load on a central server. The system scales gracefully.

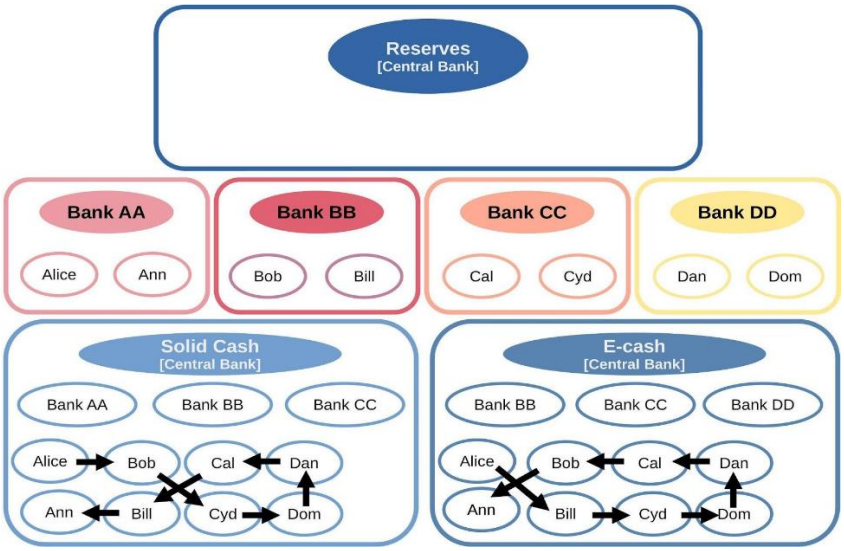
Figure 8: Cash Payments



Cash payments are directly between the parties without intermediaries both for E-cash and Solid Cash. The central bank is a guarantor of the currency used in both cases. E-cash payments can be local or remote.

Transferable payments are shown in Figure 9. With Solid Cash and E-Cash, any payment received can be immediately paid to another party, without delay or restriction. This is an important property for resilience and scalability.

Figure 9: Transferable Payments



E-cash Performance - Privacy, Security, Scalability, Resilience

In a system with offline store of value, privacy is an inherent property of the system: by default, by design. Only those details that are intentionally sent to the system operator are visible. In the case of Digital Public Money, no information about the payer in any transaction is ever returned. Cryptographic blinding operations insure the integrity of the system without revealing the identity. The identity of the payee is replaced in each transaction, with a mapping retained in a distinct system, available only following appropriate judicial review. The identity of the payee can never be determined from the system logs. The logs contain complete transaction information, so AML and taxation compliance can be validated. Since no identity information about the payer is retained, privacy is guaranteed. Payee privacy is maintained, but can be unmasked if evidence of fraud is detected.

A system based on individual offline store of value is inherently more secure, more scalable and more resilient. With modern hardware, distributed systems are highly resistant to remote attacks. Individual stores must be physically stolen and attacked, one at a time.

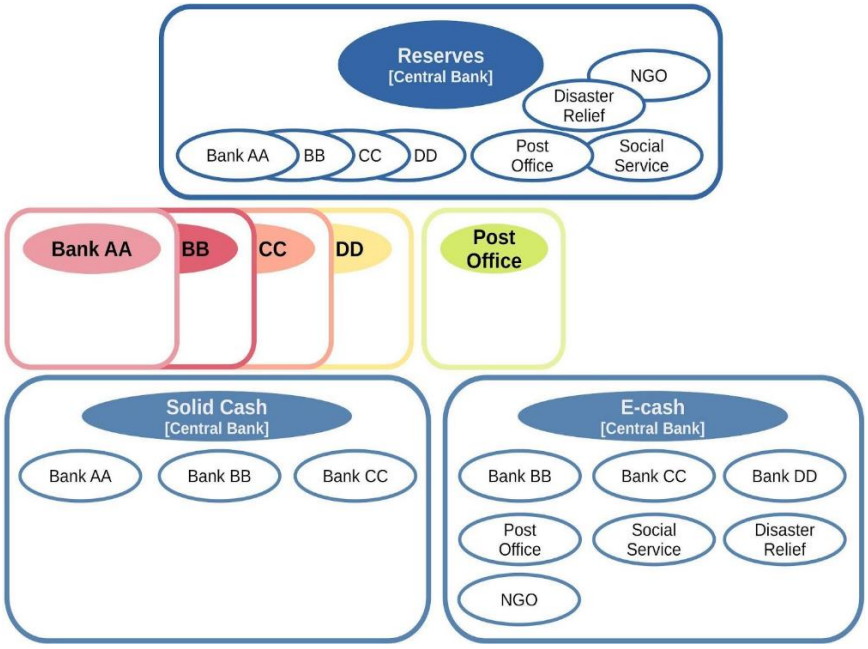
This is slow and prohibitively expensive for attackers. Even for state actors where cost is no object, the logistics are challenging and the time required will allow the system operator

time to detect and respond. By contrast, a centralized ledger presents an attractive target for attackers. Large sums can be comprised with a single attack.

An offline system scales naturally. Every additional E-purse deployed adds to the system capacity for simultaneous transactions. There is never a need for an online real-time connection to complete a payment. It is also inherently resilient with no central point of failure for transactions.

E-cash can be distributed through banks like Solid Cash, as shown on Page 4. It can also be distributed through other agencies approved by the central bank as shown in Figure 10.

Figure 10: E-cash distribution beyond banks



There are scenarios where E-cash needs to be distributed to populations who may not hold bank accounts. This can be easily and securely facilitated with a simpler arrangement than a full banking license (e.g. Post Offices, social service agencies, disaster relief organizations, and other NGOs.) Figure 10 shows the Post Office hosting a form of public bank account, while the other organizations operate exclusively with E-cash.

As guarantor, the central bank is present in every transaction. To ensure the integrity of the system, the central bank receives complete information, including transaction information, without identity details, and aggregates suitable for managing the money supply and the economy. E-cash improves the information available to the central bank and to economists, compared to Solid Cash.

Conclusion

By implementing Digital Public Money as E-cash, everyone benefits. The users: individuals, corporations, retailers, small businesses, banks, and others get the benefits of digital money without having to sacrifice their privacy, to subject themselves to 3rd party

monetization, and without having to pay exorbitant fees. Basic payments can be completely free from fees. The system operator does not have to build and operate expensive online real-time systems at scale. The incremental cost of one E-purse to E-purse payment is very close to zero.

An E-cash system based on an offline store of value supporting offline payment addresses the requirements for all CBDC stakeholders: individuals, retailers, businesses, financial service providers, the central bank, the government, and academia. It is digital money for the public good.

In addition to the basic benefits like payment over the internet and fast retail payments, additional value added services can be built on top of the system. With careful design, Digital Public Money can be made impossible to steal by ensuring every transaction completes to the desired payee. E-cash can significantly reduce the cost both of cash handling, and of Private Money fees, while protecting the privacy of the participants. offline E-cash is inherently private, secure, scalable, and resilient.

It’s time for central banks to deliver offline E-cash: to deliver Digital Public Money.