Digital Public Money Infrastructure (DPMI), University of Manchester
Working Paper No. 3

Cash: The once and future king

Eduard de Jong
Visiting Research Fellow, University of Manchester

15th May 2026 (version 2.0)

Abstract

Over the last 30 years most financial services moved to the digital realm using centralised account ledgers operated by commercial entities. These digital form of money bring credit risk, imply the use of third party infrastructure with single points of failure, exclude parts of society and struggle to protect privacy. Clearly, there exists an as yet unmet need for a digital form of money that does no suffer from these defects. This paper meets that challenge. It presents a robust, distributed, digital system to implement a digital bearer payment instrument: digital public money (DPM). It shows how DPM, based on a unique technology, aggregating receipt tokens (ARTs), is a form of money accessible to all for a wide range of payments. DPM is better than cash or bank accounts in meeting the needs of the digital age: it supports both online and offline payments, sub-second instantaneously transactions, protection against impersonation fraud, resilience, high transaction capacity and support for concurrently receiving and making payments. No proposal currently discussed for a CBDC can bring those benefits in this unified way to all in society. As digital **public** money, the monetary value as DPM is issued by the central bank. The central bank plays a key role in ensuring integrity of the issued money and protecting its value in transit between payer and payee. The central bank also assures direct ownership of DPM by provisioning users with the essential secure operational part of a digital bearer payment instrument. Ten different use cases are described to highlight how different players in the economy can specifically benefit from using DPM.

Keywords: digital public money, electronic cash, direct ownership, digital payment, reloadable banknote, formal model.
JEL codes: .

1 Introduction

"*Cash is King*" is the traditional expression that, if you intend to buy anything, offering a payment in cash will be key in convincing a seller to accept your price: accepted cash can be spend directly or stored for later. There is no credit risk. Can in a digital world cash be *King* again?

A resounding *Yes* is the answer to this question presented in this paper. It explains how a digital form of money can be created that users can experience in a payment both as payer and as payee, in closely the same way as using physical objects. Additionally it demonstrates how money can actually be implemented digitally for use by anyone as a digital bearer instrument to securely make payments over any distance. This digital money is held in *direct ownership*, just like cash.

Digital money with direct ownership expands the concept of electronic cash (e-cash). Van Hove presents an analysis[19] of deployments around the

turn of the century in many countries in Europe of e-cash systems, including Danmønt in Danemark, Geldkarte in Germany and Mondex[22] in the UK. E-cash is digital information stored in a secure processor chip embedded in a plastic card; embedded software implements a payment protocol. The protocol enables an offline digital payment as a transfer of monetary value directly between the devices operated by payer and payee. E-cash did offer a form of direct ownership of digital money, constrained by the fact that it could only be paid to merchants. This paper presents unconstrained direct ownership of digital money that can be used in a payment with a balance transfer protocol.

The challenge how to protect an offline payment with cryptography has be taken up by many, especially under the additional condition that identity of the parties operating the devices used should not be disclosed by information exchanged in the payment protocol. Cryptographer David Chaum published a seminal paper in 1982 [8] on the implementation of privacy protecting digital money. Over a hundred papers followed and several hundreds of granted payments. These cryptographic solutions are based on a metalist model of money: the use of a digital equivalent of a coin or banknote. Such protocols inherently suffer from a special form of replay attack called "double spend." The idempotent payment protocol in this paper is based on a balance transfer and is imune to replay attacks.

There exists abundant literature on digital money as crypto currency, discussing various distributed implementations of an online central ledger for its implementation. A payment in crypto currency utilises an intermediation automaton to maintain integrity of its ledger. This paper presents storing and using digital money offline, with integrity of the money protected by distributed dedicated secure processing devices, physically secured electronic devices (e-vaults), each operated by the owner of the money it stores.

The 2023 report[14] by the BIS Polaris project with a review of available products offering offline payments found that all of them required post–payment inspection to detect a potential loss of value due to loss of communication. Repairing this fundamental operational defect in these existing products is addressed by tight integration with an account–based money implementation system. The idempotent payment protocol in the secure implementation of money presented in this paper results in an operationally self contained system.

In 2021 Bindseil et al. identify potential uses case for CBDC[2, p. 16] as consumer–to–consumer (C2C), physical point of inter- action (POI), E–commerce, recurrent payments and corporate/business to business (B2B). The Digital Public–Money Infrastructure (DPMI) presented in this paper realises CBDC with DPM to support all these use cases.

The requirement for a CBDC to be cash–like is reported by the ECB [23, p. 9], and other reports [7, 10], in particular for its adoption. Bindseil et al. in [2, p. 30] present further requirements. DPM with direct ownership is clearly cash–like; it can meet all other requirements.

A 1996 report by the BIS CPMI[3] on security in a smart–card based e-cash system recommends to set limits on the amount of digital money held and paid. In a DPMI physical security for holding digital money in an e-vaults is scalable to to protect any amount a user could require. Operational security in DPMI is actively and adaptably managed and to the user DPM appears as effectively unconstrained. Applying active managemt and scalability to security in a digital implementation of money is novel.

1.1 King cash in battle

In a Welsh legend, dating from the early European middle ages, a king, named Arthur, successfully, through a number of battles he won, brought safety, stability and prosperity to parts of what we currently know as England and Wales. Years later, after his death from receiving fatal wounds in a battle against his incestuous bastard son, turbulent and uncertain times in these parts resumed. The legend further tells[1] us that King Arthur will, at some time in the future, return to restore order and bring renewed prosperity.

During its over two and a half thousand year long reign, King Cash enabled marketplaces around the globe to trade in a wide range of goods, with customers and traders both local and from far away. In this way king Cash brought prosperity to communities large and small.

In our times, in a competition with electronic payments enabled by banking card, crypto currencies, stable coins and tokenised assets King Cash, in some way, is in a battle[12] too.

This paper presents how in a digital, partially immaterial form, money can again become a common good.

1.2 The digital return of the king

This paper is organised as follows: The next section, section 2, presents the challenges for a digital implementation of money by reviewing its positive and negative properties. The positive properties include universality, immediacy, privacy, low costs and lack of credit risk.

Section 3 paints a future society with a digital form of money issued by a central bank universally available for all in society. It presents a DPMI wherein digital public money meets the challenges public money in section 2. An overview of ten use cases shows how the benefits of using public money in digital form can be available to a wide range of members of society.

Section 4 presents a generic formal model of money as an information system. This model is the basis for a provably correct design and implementation of DPM. Section 5 builds on the previous section to show how ART technology enables the implementation of DPM. It presents a formal model of this implementation by extending the generic model. This model shows the operational correctness of the offline computation at the heart of a digital payment that uses ARTs as personalised, reusable, balance tokens. This payment computation is executed within the secure confines of a hardware balance token, the payer's e-vault. A summary of DPM operational features in comparison with those of cash and bank accounts, shows DPM as a superior system of money and payments.

The final, concluding section shows that as a Digital Public–Money Infrastructure, in which digital money is issued as public money, as digital cash, like King Arthur of the legend,

King Cash will return!

2 King Cash

A merchant prefers accepting cash as the alternative is either to give credit or have no sale. For many centuries, giving credit used to be the main way for

[1] In 1958 T.H. White published a retelling of this legend under the title "*Arthur: the once and future king*[21]"

merchants to retain customers, this credit was then, at regular times settled in cash, typically coinciding with the payment of wages.

To give credit the seller needs to know the buyer. This knowledge enables an estimate the risk of losing money.

Cash, on the other hand gives the seller strong confidence in the absence of risk.[2] Hence, for a very long time in human history, payment in cash has been the much preferred way to receive payment. In the digital era electronic payment system are being presented as forms of cash, as coins, as gold, or as cash-like, while these system are all based on commercial entities maintaining accounts with private money for users.

Before the modern age, cash was the main way for customers to pay without an a-prior trust relationship with a merchant, e.g. being local. Still, in 2026 cash is the main means of payment in many countries around the world, especially in rural regions.

The main features of cash:

1. Cash has a recognisable value, the receiver of cash knows it can therefor spend that same value[3] in the future;
2. Ownership of cash is direct, possession means ownership as it gives the owner full control of when to spend, how much to spend, and who to pay;
3. Payment in cash is instantaneous, every piece of cash, whether coins or banknotes, handed over to a payee changes ownership at that very moment;
4. Cash payments have no fees, anyone paying or being paid with cash only requires the exact amount involved;
5. Payment in cash involves only two parties, it is finished there and then, and no other party is directly involved in the transaction;
6. Payment in cash is irrevocable, there is no way to retrieve the value paid;[4]
7. A value paid in cash has no memory of its previous owner(s), so the payer does not need to be known and could be anonymous;
8. The ability to pay is only constrained by the amount of value owned and not, for instance, by arbitrary limitations;
9. Knowledge of the amount of monetary value owned is exclusive to the owner.

The drawbacks of using cash:

a) Storing cash entails the risk of theft, it needs physical and organisational protective measures with a strength appropriate for the amount being stored;
b) An amount of cash can be bulky, even at relative low value, which limits the amount that can practically stored, or used in payment without adding costs;

[2] Aggietta and Orle´an analyse[1] the various aspects of the trust in money that provides the basis for the perceived minimal risk in cash. Brunton, in the first chapter of his book "Digital cash"[4] argues that a key characteristic of money is precisely the trust in the future use as a value. Complementing these descriptions, in his PhD thesis[20], Walton investigates the perception of trust in money by its users, particularly in digital forms.

[3] As a related but separate issue, the *monetary system* in which cash is being issued and used is concerned with providing trust that the same monetary value carried as cash can at a later time pay for about the same amount of goods or services.

[4] Cash is a face to face transaction and any mistakes in a payment can easily be detected and corrected. reclaiming a payment at a later time, e.g. in a court of law, is hard as a cash payment does not leave a trace.

c) Creating a receipt for a cash payment is a separate operation for the payee, as is receiving the receipt by the payer, which both might not be possible;
d) Cash facilitates laundering money.

3 Digital Public Money with direct Ownership

Like cash, digital public money (DPM) is owned directly by its user: A user determines when to spend money, how much of it and who will be the receiver of that money. The digital payment is a private affair, only involving payer and payee.

DPM is public good; it can be used by anyone to hold or to make a payment or receive one. An amount of DPM received in a payment is under the exclusive control of the receiver, individual, business or government agency to spend it in a payment at an undetermined future time The payment is gratis, it involves only the payer and payee, who exchange two digital messages to complete it.[5]

In DPM a payment consists of two digital messages. They can be sent in any form, over the internet, via near–field–communication (NFC), as QR codes, included in email, or any combination of these different means of digital communication that might be conveniently accessible by payer and payee The physical distance between payer and payee has no impact on the ability to pay or receive DPM.

The amount to pay also has no effect on the ability to make a DPM a payment, it is just a digital number in the messages exchanged between payer and payee. The DPMI leverages the digital nature of the payment to automatically select, from the set of installed cryptographic protection algorithms and keys, a pair that has been pre-qualified as appropriate for the value.

Transmission of the two DPM messages has no specific requirements. Both contain an ART, which is a self contained digitally signed data structure that guarantees authenticity and integrity. The first message may additionally contain payment related data the content of which will have been established prior to the payment. The ART does contain a cryptographically generated pseudonymous reference to the payee. The payer is either anonymous or pseudonymous. The need for transport protection for confidentiality depends on the use case, transport layer security (TLS) could be used in some.

3.1 The e-purse and e-vault

To own and use DPM *e-purse* software is required, which access software embedded in an e-vault.

The e-vault is specifically designed to hold digital money; it is a specially manufactured, small computer dedicated to protect integrity of the public money it contains and personalised for the owner of this money. It communicates contactless, via Bluetooth, NFC or other suitably secure channel, with the e-purse software installed on a personal device of the owner of the digital money.

[5]For a digital payment over a distance users of digital public money will need have a digital communication infrastructure available. using such an infrastructure will incur costs, which, however, is often negligible.

The e-vault provides *direct ownership* of money. The e-purse software provides the user interface and manages communication. A user registers their e-vault with one or more (personal) devices running the e-purse software. In a payment the e-purse communicate with e-purses in other user devices; access to biometric user verification provided by the payers device may be used to establish intent.

Current ubiquitous availability makes a mobile device, phones or tablets, the obvious direct ownership companion device for each e-vault.[6] The e-vault is cryptographically tied to it's owners mobile device, there could be more than one. This secure device–to–device binding is renewed regularly. The binding is established via NFC connection. The e-vault provides a button to securely establish user intent for this security operation.[7]

Figure 1 presents this two–device model for using DPM with direct ownership, showing the two messages exchanged between the two e-purses in a digital payment[8] Just like cash, this payment only involves the payer and payee. The e-vault is a custodial device that stores money digitally together with the cryptographic keys to validate an outgoing payment and the software that implements the payment protocol. The e-purse is the complementary trusted software in a personal device that has been given secure access to the payment function in the e-vault.

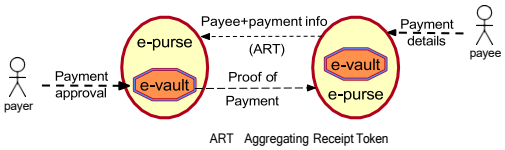

Figure 1—*The e-vault as integral part of a user's e-purse.*

The phone with its e-purse app and the e-vault are the digital equivalent of a user's wallet with a banknote: the wallet must be opened to access the value of banknote. Carrying this metaphor a bit further, the e-vault can be seen as a reloadable digital banknote. Issuing an e-vault can be done by selling it to its prospective user for the value it stores, similar to how users buy banknotes.

Making a digital payment involves an intentional user/owner ceremony with the mobile phone while it presents payment details to its owner. The e-purse app could ask for explicit approval for amounts over a configured limit; for lower amounts it could derive implicit authorisation from the movement of the phone, e.g. tap a POS terminal to pay with the NFC.

3.2 A custodial device as security anchor

Digital money is invisible. The main way for a human to experience it would be as messages on a computer screen. A printed statement provided by a trusted source, like a bank statement, is another way to experience invisible, digital money.

DPM meets this user=experience challenge by providing something tangible, an e-vault, that physically represents owned monetary value; branding

[6]Earlier attempts to provide a digital forms of cash, like Mondex in the late nineteen nineties, required dedicated devices with a very basic user interface only supporting face–to–face payment.

[7]Other solutions for securely setting the e-vault configuration exist to meet specific operational conditions.

[8]The figure does show how the payer interacts with the e-vault via the e-purse to approve a payment, while the payee interacts only with the e-purse software to initiate and receive money digitally. Further details of the idempotent DPM, two-message payment protocol schematically shown in fig. 1 are provided in section 5.

and artwork on that device could reinforce the meaning of money, like it does for a banknote.[9]

The e-vault makes owning digital money visible. Its tamper-detecting secure enclosure, the proven-correct implementation of the payment software inside and its provenance, e.g. issued by a central bank, makes it a trustable custodian of money. Experience by using an e-purse to make and receive payment, and continuously doing so, and seeing others doing so, confirms the trust in the DPM owned in one's e-vault.

As a custodial device an e-vault serves two masters:

I) The owner of the money, with exclusive control of spending funds;
II) The issuer, typically a central bank, with strongly protecting the integrity of the money stored and transmitted.

Irrespective of the physical form, the design of an e-vault prevents extracting money without owner authorisation:[10] Tamper detection in the device will disable the payment function when triggered.[11]

System security for the DPMI is actively managed. Security management is based on capabilities[18] and an e-purses regularly contacts system operator servers to refresh these. Two types of capabilities are used securing outgoing and incoming payments, respectively.

An ART is a capability to receive payments, securely configurable with an expiry date, a maximum number of payments or the maximum amount in each payment. Payee information or information on a special kind of payment intended to be presented to the payer when authorising a payment could be added to this secure configuration.

An e-vault typically has multiple secret payment keys available to secure outgoing money. The digital certificates that allow to validate a payment from an e-vault are capabilities for making payments. Digital certificates are configured with an expiry date and the maximum and minimum amount of a payment; certificates for payment keys with the same value range typically have staggered expiration dates.[12] To protect payer identity blinding can be used in securing the certificates for keys configured suitable for use in consumer payments.[13]

The e-purse is programmed to be adaptable in managing capabilities. In this way, a user, in its daily use, would not notice the active management of system security.

With managed capabilities potential attackers, however, will discover that their efforts, because of limitations imposed by capabilities, cannot cause any significant harm, severely constraining possible extractable value.

In a request from the e-purse to refresh capabilities, any expired ARTs will be submitted to the system operator. The transaction history recorded in each ART provides the operator with a source operational data. User privacy is protected when analysing this data as an ART is pseudonymous, it does not directly identify its user. The pseudonymous operational data is used to validate use of payment keys as conforming to their configuration. It can be

[9]Like a banknote, form and appearance of an e-vault could be protected by law.

[10]Like any secure device the costs of implementing and maintaining security in an e-vault has to be balanced with the risk being protected. The e-vault can be implemented in different security classes.

[11]Unless physically severely compromised, money can be recovered from a disabled e-vault by issuer accredited service provides.

[12]The key size and cryptographic algorithm used to secure payment key certificate can be chosen to match the configured value range.

[13]In any payments where a payer has an interest to be known by the payee, the payer can include a hash of identity information in the data signed by the payment key.

used to compile distributions of the frequency and value of payments or the velocity of money. The pseudonymous data can be retained to compile other statistically interesting data about the monetary system.[14]

The enforcement of Anti Money Laundering (AML) rules in the use of DPM is enabled by the availability of pseudonymous statistic payment data. The operator can apply filtering, e.g. based on AI, to detect patterns in the flow of money over time that might point to a movement of dirty money. This detailed analysis of payment patterns over a long period has the potential to be able in identifying AML perpetrators. It is likely to be more effective than the current costly and intrusive approach.

The e-vaults are the distributed anchors for the security in a DPMI, like banknotes are for cash. With no sigle point of failure, and actively managed security, the DPMI can be a more convenient and secure system of money and payments than cash.

Acronyms and Definitions

DPM: Digital public money is held in direct ownership, spendable in a direct communication of any type between payer and payee.

e-purse: An electronic purse is the software used by the owner of DPM to access it for spending or receiving and to integrate DPM payment operations in an IT system.

e-vault: A secure custodial device to hold a balance in DPM, maintain the integrity of money in a payment and to provide secure, exclusive spending control to the owner of the money.

ART: An aggregating receipt token is a cryptographically sealed, expandable digital information token with an immutable balance value, that is used to transport DPM from the payer e-vault to the payee e-vault in multiple payments to the same payee.

DPMI: The Digital Public–Money Infrastructure comprises all e-vaults used by owners of DPM and any further operational components needed to securely operate a large–scale system of digital money as a public good accessible by all.

3.3 E-purses galore

Anyone in society can own an e-vault and operate one or more e-purses to hold DPM and access it to make and receive payments. The e-purses can be integrated in the users Information Technology (IT) environment.

The physical security for the e-vault can be adapted to its intended use. It could be more heavier, more bulky and attachable to a surface to prevent it being taken hostage. Or it could be placed inside a high secure environment, e.g in a cage in a compute center.

An e-purse can be used by individuals, banks, merchants, households, small and medium–size enterprises (SMEs), corporations, financial institutions, Payment Service Providers (PSPs), tax authorities and central banks.

[14] The use of configurable capabilities provides the operator with a tool to tune the operational balance between privacy protection and system integrity.

For each of these ten different users a brief description is presented below to show how the user in these cases could benefit from the direct access to public money in digital form provided by DPM.

These descriptions reference details of the implementation of DPM with matched, personalised software and hardware, with e-vaults and ARTs. Section 5 describes details of these different types of monetary balance tokens.[15]

The use cases below show how DPM benefits society: with effectively zero costs of payments, high resilience, unbound capacity, effective AML and, for its users, high security, fast processes with low complexity and low operational costs, and protection of privacy.

Individuals

By far the largest group of users by number in a DPMI are individuals;[16] their e-purse uses a portable e-vault with copies of its software installed on one or more personal devices, like a mobile phone, tablet, laptop or desktop computer.[17]

A portable e-vault can be manufactured in several form factors to match different user preferences: e.g. pendant, key fob or thick distinctively shaped coin. Each form of an e-vault has to accommodate tamper detecting features, a battery, antennas and a few embedded processing chips. These separate processors are for the secure processing of the payment related functions, tamper detection, external communication and harvesting energy from WiFi and NFC to charge the battery. A Java Card™ chip would be very suitable as the security chip embedded in an e-vault; using such a smartcard chip would provide a very strong layered defense.[18]

The personal e-vault can implements a "*find me*" mechanism, which would be triggered when losing communication with the user's smartphone. The "*find me*" app on a mobile phone can then locate the portable e-vault where it was dropped.

The initial deployment of DPMI can be structured regionally, involving campaigns with face–to–face interactions with potential users and assisting them to install the e-purse software. A special e-purse-based issuing terminal, typically a tablet, is used to securely initialise and personalise a new e-vault before handing it over to a user.[19].

Deployment of individual e-purses in a region could be scheduled after deployments to shops and in banks that serve potential local users and, specifically, shop owners. The physical nature of the e-vault enables such a gradual, controlled, regional deployment of the DPMI.

[15]That section specifies, at an abstract level, how these two types of tokenised money, the e-vault as a physical one, and the ART as a logical one, together can correctly implement money with secure payments over any distance with immediate finality without intermediation.

[16]In the EU the number of individual users could be over 400 million.

[17]The functional requirements for this personal device are moderate. A cheap, minimal configuration device could be made available in countries, or regions, with a low mobile phone deployment rate.

[18]The generic security objective in the design of an IT system to implement a DPMI is to assure that an attacker has no effective way to profit. Such a design includes detection, isolation and limiting damage.

[19]A range of different deployment scenarios can be designed to meet local conditions and user expectations.

Banks

Commercial banks play a crucial role in the economy, they provide accounts to individuals and companies and issue mortgages and other loans. They are also an essential link in the monetary system enabling a central bank to manage the amount of money in circulation.

In the DPMI commercial banks continue to play these essential roles: A bank owns DPM and operates an e-purse integrated in its IT system. The e-vault that holds the bank's DPM could be implemented as a industry standard Hardware Security Module (HSM), that has been provide via the central bank and initialised with essentially the same digital money software as in its portable cousin. This HSM could be securely hosted in the bank's secure data center. The bank balance sheet shows the amount of DPM in the e-vault as *digital cash at hand*.

The central bank can make payments to a bank from its own pile of DPMfootnoteAs the issuer of DPM a central bank operates a specially modified e-vault as part of a dedicated issuing e-purse. Additional e-purses could be used for operational purposes, like provisioning liquidity. in the context of its liquidity provisioning arrangements, either as a withdrawal from the banks reserve account or it could be against a credit line. An account holder making a deposit is another way for a bank to receive DPM.

An account holder can withdraw from its account in DPM; the bank can deposit DPM on its reserve account. Both these operations reduce the bank's *digital cash at hand*. Deposits and withdrawal in DPM can be completed in under a second with instantaneous finality; they could be made multiple times a day, the frequency would, likely, be subject to contractual arrangements.

Deposits and withdrawals are DPM payments that use ARTs configured with the number of the account to receive or to provide the money. A deposit ART will have been created specifically for the bank, it securely identifies both the bank's e-vault as receiver and the depositor account to be credited. This ART is for exclusive use by the account holder and is stored in its e-purse; the bank, after receiving a payment with this ART, uses it to simultaneously update the value of its e-vault and the account holder database.[20]

A withdrawal is a payment request from the account holder, which includes one of its ARTs that has been configured with an account number. An account holder's e-vault can be enhanced with a secure withdrawal authorisation function configured for acceptance by the bank involved. This function can provide a cryptographic proof for the withdrawal request as originating from the account holder.[21] By validating the authorisation data generated by the account holder's e-vault, the bank's e-purse accepts this request as a payment authorised by its owner to then make the user requested DPM payment. The proof of payment generated by the bank's e-vault as a withdrawal in DPM can be processed by the bank database as undeniable record of an authorised payment.[22]

Commercial banks play an essential role in the distribution of DPM by providing deposits and withdrawals by users combined with their direct ac-

[20]Abuse of deposits, e.g. to circumvent AML enforcement, could be provided, for example, by issuing a special payment key configured for deposits over a certain amount.

[21]The EMV JavaCard applet could be used as the model to implement this function in an e-vault. Doing so could render an e-purse into a universal digital payment tool that also supports EMV payments.

[22]Storing the digital signature and other payment details in the database facilitates auditing the two corresponding flows of money.

cess to DPM at a central bank, Just like they did, an will continue to do, in cash.

Automatic Teller Machines (ATMs) complement the integration of DPM in the financial system. They provide cash–to–DPM and DPM–to-cash services local to where cash will be used. An ATM can issue banknotes on receiving a payment in DPM, the ART to use for this payment could be displayed as QR code (QR) code and the proof of payment delivered via NFC by tapping a phone. An ATM that can accept cash could convert the received amount into DPM by making a payment using an ART provided via NFC with the proof of the DPM payment presented as QR on the ATM screen.[23]

Using DPM to pay enhances privacy protection as the payee does not learn customer data form the payment, it is not needed for a secure payment.

Merchants

A shop can use its e-purse to accept customer payments; the payment acceptance component of the e-purse software can be installed in each of the merchant's POS terminals. All these terminals can accept payments at the same time, irrespective of their number. To support merchants with POS terminals at check-outs, the e-purse software includes an ART provisioning component, that regularly communicates with a configured set of terminals.

The main part of a merchant e-purse, including its e-vault, could installed in a back office. The e-vault will be build with a security level suitable to hold a daily revenue intake and could be bolted to the wall or otherwise protected from being taken unnoticed. After redeeming the ARTs that have collected the receipts of the day, a merchant can than order fresh supplies and immediately pay their various suppliers from these receipts.

The effectively zero costs of receiving and making payments in DPM will reduce costs of merchants. All parties in the logistic chain can benefit from faster, more secure zero–cost payments in DPM. These logistics benefits will be a driver for adoption of DPM.

Households

A household can have a joint e-purse for use by all its members; the e-vault in this e-purse, like the one for merchants, will be built stronger than a personal e-vault, and could also be fixed to the house. Wages earned by household members would be paid into the joint e-purse, shared costs, rent or mortgage, energy and other duties, can be paid out of the DPM it holds. The e-purse software supports scheduling recurrent payments.

Individual e-purses for household members can be topped up regularly, e.g. daily, even remotely, from the money in the shared e-vault. The e-purse software keeps track of these money flows. Kids could have pocket money allocated with a daily allowance transferred to a junior version of an e-purse.

SMEs

The e-purse for SMEs are integrated in their administrative software package. Depending on the amounts stored and paid the company e-vault could be stored in a back office. Service providers could offer an alternative with secure, dedicated hosting facilities to physically protect e-vaults.

[23] An e-vault to hold the funds payed out by an ATM against receiving cash could be located remotely.

Such a facility could provide round–the–clock secure physical access to the e-vaults for its customers while also providing direct digital access by its owner to each device and the digital money it contains, e.g. each protected by a different virtual private network (VPN) channel. Physical access to the e-vault would be used to securely manage personal devices to configure them for (continued) access to an e-vault to authorise payments with its.

The company e-purse receive business revenues and pays expenses: employees, suppliers and service providers etc.. The e-purse software supports cash management with cash sweeps and timely withdrawals to make planned payments. Invoices can be prepared to include a QR code with the ART to use to pay.

Corporations

A corporate e-purse software is integrated in its IT (cloud) infrastructure; requesting and receiving payments are software functions that are seamlessly integrated in business software. A proof of payment received from payer can directly be recorded in a database as an update to accounts receivable; a proof of payment generated for an outgoing payment can be recorded in a database transaction to update accounts payable. This cryptographic proofs establish verifiable facts and can be shared with any department that might need to now about the payment, e.g. (external) accountants.

The authorisation for a business payment can be given via a mobile phone used by an authorised employee; multiple such employees could be recorded in an e-vault, possibly with different authorisations.[24] The payment authorisation structure can also reflect the geographic and logical governance structure. A company CFO would be recorded in the e-vault as the authority for delegating these payment authorisations.

A corporate e-vault could be realised as an industry standard HSM that has been manufactured in accordance with central bank and initialised by it for actively managing its security during use. Multiple HSMs could be deployed to support multiple currencies.[25]

Operationally, a corporate HSM could be hosted by a service provider, e.g. their cloud provider, which could provide a secure local access point, with a pre–established secure connection to the e-vault, to be installed in an CFO office to support secure authorisation management.

Financial institutions

A financial institution is a corporation that can act as part of the monetary system offering products and services It manages digital assets, provides a market place for them or is a market maker. Frequently making and receiving payments is essential in most of its operational activities.

The use of DPM with its atomic transfer of monetary value over any distance will bring clear limits to when an initiated payment will be final

[24] A corporation could create different sets of ARTs for different types of payments it uses in its administration. An employee authorisation could then refer to a particular payment type encoded in the ART configuration.

[25] Central banks could reach agreement between them on a common comprehensive set of detailed operational specifications and the security evaluations to be applied to HSMs. These specifications could include implementing secure operational partitioning software, e.g. conforming to the Java Card specs. With partitioning software, an HSM built in accordance with these shared specifications could be used by different central banks to each install and configure their own e-vault in a shared physically secure device. Doing so could reduce (operational) costs for corporations of owning multiple different currencies, making then available to more users.

as it enables digital, atomic Delivery-versus-Payment (DvP) and payment–versus–payment (PvP) in public money.

The corporate e-purse owned by a financial institution can make payments in any amount and in a high volume, it could also be configured to simultaneously accept a high number of payments, as presented above for merchants. Each payment is in itself instantaneously final and can include cryptographically secured transaction details.

The cryptographic proof of each digital payment provided by the ART, used to transport the money and associated payment detail, enables the deployment of trusted an autonomously operating, automaton that implements the atomic transfer of (digital) ownership: DvP e.g. for shares, bonds and other financial instruments; PvP e.g. for currency exchange.[26]

Banks and other financial institutions could migrate their retail payment operations to the DPMI, as users can withdraw DPM to make their payments directly to payees and deposit any DPM after receiving it. Since a withdrawal is a payment to the same person or legal entity, AML would be a lot simpler, reducing costs of supporting retail payments. Enabled by DPM, the issuance of digital (retail) bonds as a saving product that is tradable in a digital market place[27] could be a way to attract funding from consumers.

Payment Service Providers

A PSP provides additional services to users participating in a payment, primarily giving credit to consumers at the POS, possibly complemented with dispute resolution, insurance, enhanced warranty and charge back. These services can be provided for payments in DPM.

A financial institution or other corporation can offer these services using their e-purse to make and receive any related payments.

An e-vault supports making multiple payments at the same time. Such a payment takes multiple ARTs as input and produces multiple proofs of payment as result, one for each ART in the input. This multi–payment process is atomic, all are either done or none of them. A PSP can leverage this technical feature to receive payments for fees for the payment related services it offers. The service payment is then made at the same time as the payment for the product or service that a payment service applies to, and only if the main payment has actually been made.

To add a service to a payment the e-purse for the payee stores ARTs for the PSP configured with its customer id. In a service enhanced payment the PSP and the seller's ART are sent to the payer. The payer's e-vault atomically computes proofs of both payments which then get sent to the payee. At a convenient later point in time the payee's e-purse software would send the PSP its updated ART. The payer's e-purse retains a copy of the PSP's proof of payment to use in a possible claim. A software extension can be securely installed in an e-vault, configured by the PSP, that could automatically compute the fee due for a service from the payment amount.

Consumer credit to be provided by a PSP at the POS can be realised as a function in the e-purse. After receiving the payee's ART in a payment

[26] Financial instruments can be implemented digitally as sealed asset–information tokens (SAITs), securely sealed by a digital signature that binds value to its owner, just like an ART binds received money to a payee. SAITs can be stored, and backed up on computers operated by their owners. Details on using a DvP automaton for asset trades are presented in my 2025 paper[17]

[27] See [17] for a way to implement a digital market place for such trades based on a DvP automaton.

request, in order to claim credit, the payer forwards it to the PSP for actual payment. The PSP can operate the token factory for the payee's ARTs to enable receiving a payment by credit to known merchants; a fee could be charged for manufacturing these specific ARTs.

The credit providing PSP can implement an atomic PvP mechanism to automate paying a payee on behalf of one of its customers. The cryptographic proof payment in DPM for the payer's fee to the PSP is used as the authorisation for the PSP's e-vault to trigger the credit–agreement–backed payment to the payee. The authorising payment also uses an ART configured with a customer id for the payer, the fee amount could be computed by an e-vault software extension configured with PSP details. The secure extension could also support post–payment of PSP fees by authenticating the payer to the PSP.

A token factory operated by the PSP could guarantee that the customer asking for a payment against its credit line is a know customer.

Providing credit at the point of sale, done with DPM, will be automatic, fully digital and highly secure and fast W. The merchant obtains payment instantaneously; and the PSP could receive its merchant and customer fees upfront.

Tax authority

A corporate e-purse of a tax authority can be used to distribute ARTs to any tax payer, e.g. after having received a digitally filed tax declaration. This ART could then be used to pay the tax due, all at once or in multiple instalments. The scheduling function in the payer's e-purse enables such installments. The tax payment ARTs are configured to identify each payer.

The tax payment ART could also be used to pay taxes due at the same time as a taxable payment. For instance, when paying wages to an employee income tax could be withheld in the same payment. Or, when receiving a payment for a sale, sales tax can be paid directly. The payment of tax in addition to the amount includes any data required by the authorities for a particular type of payment.

Event–based tax payments in DPM utilise a multi–payee–payment by the payer's e-purse. In that payment the tax payment ART is one of the inputs.

A software extension can be installed in an e-vault, configured by the tax authority, to automatically compute the amount of tax due from data in the taxable payment request, similar to payment for services and fees to a PSP. This extension could also be used to insert cryptographically protected event–related data in the tax payment, such as a tax id.

Direct payment of taxes in DPM would make paying and receiving taxes simpler and cheaper. It would relieve merchants and employers from keeping an administration of taxes due, and from maintaining its supported documentation.

The central banks

A central bank provides DPM to banks in payments from one of its corporate e-purses. Payments could be realised as fast withdrawal from bank reserves. A bank can make deposits to its reserves at a central bank.

The central bank also operates a special issuer's e-purse dedicated to creating and destroying DPM; payments from the specially programmed e-vault in this e-purse would be restricted to be made to the bank's corporate

e-purse. The issuing e-vault could be securely stored most of the time in an on–premise vault without data connectivity. It could then be connected briefly after having created DPM to transfer it to the corporate e-purse, which is used for the distribution of digital money to banks.

Financial institution can make direct payments between themselves in DPM. The central bank can operate the "factory" for the ARTs used by the banks; this provides information in these flows of money. Managing the configuration of these interbank ARTs creates a mechanism for a central bank to tune the velocity of money moving at this level of the financial system. This adds a tool to monetary controls.

The central bank also supervises production, distribution and initialisation of e-vaults. It contracts suppliers and service providers to actually issue a suitable e-vault to the various DPM users and supervises their operations.

A central bank could participate in a global consortium for the governance of the development of open-source software for all the components needed to deploy a DPMI for use by all in society. In addition to the generic software embedded in an e-vault and at the heart of each e-purse, the use-cases above provide a sample of the various software components that could be developed. The global governance consortium could establish criteria for trusted service providers qualified to support all parties in the DPMI.

3.4 A tale of two tokens

The benefits to society of digital public money and for all its individual, business and government users is based on the use of two types of novel monetary tokens. Both tokens have a well–protected monetary value that is maintained as a balance; using an idempotent atomic monetary value transfer protocol, their value can increase or decrease by arbitrary amounts as they are used by their owners to make and receive payments.

The tale of these two balance tokens:

i) a hardware token, the e-vault and
ii) a digitally signed, immutable yet extendable information token, the aggregating receipt token (ART);

is one of a bright, digital future of public money provided by a Digital Public–Money Infrastructure.

Each of the tokens has a different, complementary role in the implementation of a payment in the a DPMI.

- An **e-vault** makes **owning** invisible digital money tangible, visible and executable.
- An **ART** securely **transports** an immutable amount of digital money from a payer to a specific payee.

An ART transports DPM in such a way that neither payer or payee is required to be identified in payment data. Payee, payer, or any other party that might need to know about a specific payment can use software to see the amount in a specific payment, enabling the implementation of atomic payment–versus–payment and Delivery-versus-Payment.

The e-purse software makes the benefits of digital public money available to its users and to society.

4 A formal model of money

Formal modelling is a specialised discipline in software engineering that aims to establish well–based trust that software actually does what its specifica-

tion declare are intended. Formal modelling can also be used to show that software cannot misbehave when it responds to faulty inputs like from an attacker. It uses mathematical proof techniques to show that a program actually responds to input and does so correctly. It can also show that implementation choices in program code are consistent with the purpose of that program.

This section and the next present, with the aid of formal models, evidence for the soundness of the concepts presented above for the realisation of digital money with direct ownership. With provably correct properties exposed in these models, an actual implementation of digital money could be proven to be correct. Provable correctness of a sofware implementation is one of the key required elements of a security evaluation. The technical details in these section can be skipped.

A formal model is an abstract description of the system that needs to be implemented, with mathematical formulated specifications to precisely describe the key system features. The formulas express how a system evolves over time as it responds to repeated varying input data; they specify conditions for internal values that must be maintained at all times, the system *invariants*.

For software that implements a secure system, like digital money, formal modeling will be essential.

This section presents a compressed version of a generic model of money to serve as basis for a model of DPM, which will be presented in section 5.

A number of researches has applied formal modelling to digital money with direct ownership. The European Central Bank presented a formalised model of electronic money security objectives[9]. Gouda and Liu use a common formal model[11] applied to several e-cash message protocols to verify that these protocols are secure against message loss, modification and replay attacks. Butler and Yadev analyse in [5] how the Mondex e-cash system[22] detects a possible loss of value during payment. Inega, Oyama and Yasuura in [13] develop a model to compare two different e-cash protocols; they establish fundamental differences in communication and security properties between the protocols. The previous formal model work has had a narrow focus on the digital payment operation. This paper presents the basis for a model of a more comprehensive digital money system.

A more comprehensive formal model of money and its role in the monetary system with a number of different, yet complementary, implementations can be found in my forthcoming paper [16]. That paper presents formal proofs of system properties.

4.1 Money as owned balances of value

Formal model 1 specifies money as an information system with a set of numbers associated users. The numbers in this abstract model are *"balances,"* indicated as B, that each represent an amount of money owned by a user. A balance is associated with its owner u by labeling it as B_u. How a user can technically be associated with its balance B is not further specified; that association is something that a concrete implementation of a money *system* will address.

The text style used for the symbol B is an indication that its value is persistent and protected against any modification not specified in the model.[28]

[28] Implementations of money will differ in details on how to achieve these data storage properties.

One of the properties of money is as a store of value and protected persistence of data provides this. The next section presents a model that includes a monetary token T, and its information content is also persistent and protected.

Model 1: Money

$$\sum_{\text{users}} \mathsf{B}_u = M, M > 0 \tag{1}$$

$$\forall u : \mathsf{B}_u \geq 0 \tag{2}$$

$$\mathrm{P}(a, B_{\mathrm{Rob}}, B_{\mathrm{Eve}}) : \quad \text{if } \mathrm{C}(\mathrm{Rob}, a) \wedge \mathrm{A}_{\mathrm{Rob}}(a, \mathrm{Eve}) \Rightarrow \mathsf{B}'_{\mathrm{Rob}} = \mathsf{B}_{\mathrm{Rob}} - a;\ \mathsf{B}'_{\mathrm{Eve}} = \mathsf{B}_{\mathrm{Eve}} + a \tag{3}$$

$$\mathrm{C}(u, a) : \mathsf{B}_u \geq a \ '\!\!\rightarrow \{\mathit{True}, \mathit{False}\} \tag{4}$$

$$\mathrm{A}_u(a, u') : \{\mathit{True}, \mathit{False}\} \tag{5}$$

Specification (1) in model 1 shows a key invariant property of a money system: its maintained *integrity*. The integrity of an implementation of money means that the total amount of money is constant; that no money can disappear and that money can't be created out of thin air.[29]

Specification (2) defines constraints: any balance B_u is either zero or positive. The payment condition C in spec. (4) guarantees that this condition cannot be violated in a payment: the model is *consistent*.

Payment, indicated with the symbol P, in spec. (3) moves money from one owner to another. It is the main operation supported in this model of money. Money only moves if approved by its owner as specified by A in spec. (5).

The specification of the operation P defines it as a pair–wise change in the value of two balances: P affects the two balances, $\mathsf{B}_{\mathrm{Rob}}$ and $\mathsf{B}_{\mathrm{Eve}}$, where Rob is the identifier for the payer and Eve is the identifier for the payee. The change in both balances is by an amount a, with the payer balance value $\mathsf{B}_{\mathrm{Rob}}$ being reduced by a into a new value $\mathsf{B}'_{\mathrm{Rob}}$ and the payee balance $\mathsf{B}_{\mathrm{Eve}}$ being incremented by a into a new value $\mathsf{B}'_{\mathrm{Ev}}$ [30].

Specification (3) also shows that spending any part of the balance requires the explicit consent of the owner in spec. (5). In implementing money establishing owner consent requires a proper design and careful operations; section 4.2 present the two basically different possible ways for am implementation.

A balance B_u thus represents the amount of money a user u has available to spend and spec. (3) shows spending money. This amount could exist in different forms: i) as a pile of cash, ii) as an encoded as binary numbers in the database on a hard disk in an IT system operated by a bank or iii) as a binary number in a digital token.

With the amount of money in circulation constant, model 1 describes a steady state of the monetary system; issuance of money is not relevant for the purpose of this paper. In this steady state there are always some owners that have money. By making payments the distribution of monetary value

[29] In a model that includes issuance of money integrity can be specified in a more generic way.

[30] By convention the tick in B' indicates that after the computations in the formula have been done the computed value replaces the old one, $\mathsf{B}' \Rightarrow \mathsf{B}$

over the owners evolves: the model is *alive*. The specifications in model 1 describe a complete implementation of money.

4.2 Central or distributed implementation

There are two fundamentally different ways to implement the money system in model 1 system:

- A *central* system uses ledgers to record all balances B_u, with ledger management software providing the assurance that in an update to the records the system invariants (specs. (1) and (2)) are respected,
- As a *distributed* system, where each user has its own private store for its balance B_u and privately performs the authorisation A_u to allow a payment to another user to proceed.

An example of centralised money system is a bank providing a debit card payment function or a central bank with reserve accounts. The authorisation for a payment $\mathsf{A}_u(a, \text{Eve})$ is performed by a bank using a database of customers and details of the banking card they have been issued. Third parties are typically involved, e.g. Visa or Mastercard.

An example of distributed money system is cash, i.e. banknotes and coins. For this form of money, authorisation is realised one coin or banknote at a time by taking it out of a wallet and handing it over to the payee.

DPM with its direct ownership is also a distributed implementation of money. Authorisation in DPM is performed by the hardware, e.g. a biometric sensor, and software in the personal device, e.g. mobile phone, that runs the e-purse software.

5 Digital public money with aggregating receipt tokens

This section extends the formal model in section 4 in two refinement steps:

1. specify (refinement 2) the two balance tokens in DPM by introducing an additional type of balance, T, to represent ARTs and how these balance information token are used in a modified payment operation and the added *redeem* operation, which adds received digital money to the spending balance; and
2. specify (refinement 3) at a high level how software and data in the e-vault as custodial device can be structured to securely and resiliently implement DPM.

A more detailed description, below, of the payment process with ARTs serves as introduction to the formal definition of the two payment related operations in refinement 2 and then refined in refinement 3.

5.1 How to pay using an aggregating receipt token

A payment uses two different types of *balance* tokens: i) a hardware token, the e-vault and ii) a digitally signed, immutable yet extendable information token, the aggregating receipt token (ART).

The ART is used to received money in multiple payments from, typically, different payers. In each payment where an ART is used again, its value is increased by the payment amount.

Figure 2 shows operational details of the use of an ART to implement a DPM payment presented in fig. 1.

The payment function of an e-vault receives an ART from a payee with an approval from the payer. This triggers a secure computation in the e-vault

that results in an updated version of the ART: the value of its balance is increased by the payment amount.

To increase the value of an ART, it is extended using a cryptographic chain that links the extension to both its previous extension and its cryptographically sealed configuration data.

A digital signature by the secret payment key in the payer's e-vault makes the extended ART a verifiable cryptographic proof, PoP in fig. 2, that the payment that just has been made. In this proof the payee is pseudonymously referred to by information from the ART provided as input.

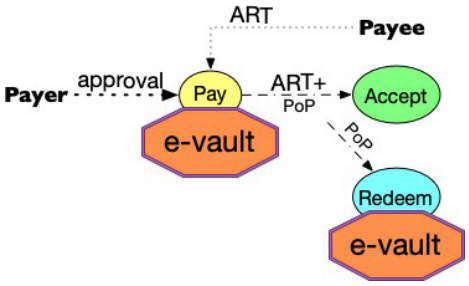

Figure 2—*A digital payment as play with two different balance tokens, an ART and an e-vault.*

The digital signature computed by software inside the e-vault makes a payment with an ART instantaneously final: the money added to that token can only be spend by the recipient; it can also no longer be spend by the payer as the balance in the e-vault is decreased by the payment amount. The payee accepts the payment with the software component in its e-purse implementing signature validation.

Acceptance of the payment by the payee can be done before the received money becomes available for spending. This operational feature of a DPM payment makes it possible to simultaneously accept many of them, like in payments at super market check outs, or bank deposits. or tax payments.

The complete end–to–end payment is done in two different operations that both involve a single e-vault interacting with the e-purse software: i) In *payment* the payer's e-purse forwards the received payment request containing an ART to its e-vault hardware to obtain an ART with an updated value as a proof of payment; and ii) In *redemption* the e-purse software of a user that previously has received one or more updated ARTs as proofs of payments presents a proof of payment to its e-vault to make money received available for future payments. Both these money operations are implemented to be idempotent: repeating any of them with the same input always gets the same result or effect.

A payment with an ART is effectively a sequence of two payments adjusting three balances: the first one gets money from a payer balance and increases the ART balance for the payee; the second one moves money from the ART balance to e-vault balance. The first balance, as cryptographic information token, can move between any two locations; the second balance, in a physical token, is at a location where its owner can have easy, secure access to it. From a security perspective easily moving an e-vault may not be desirable in many use cases.

Both tokens have balances, not a fixed value; ownership of money is changed in the first of the two balance transfers that together make form the end–to–end payment, the second one consolidates receipts for further spending.

5.2 Manufacturing aggregating receipt tokens

An ART has been specifically created for use by a particular payee; the system operator provides only services to create ARTs, operating a *token factory* can be delegated to trusted parties, like banks. There may be many differ-

ent "*token factories*" that support the DPM system, possibly adding specific information to the new tokens, which could be strongly authenticated, e.g. account numbers for depositing DPM as mentioned above in section 3.3.

The initial value of an ART is 0. It is further configured to be used for a specific number of times and up to a specific aggregate value. With a zero initial value, a token factory is not an issuer of money, its task is to created a token that is cryptographically bound to a specific e-vault as requested by the owner of its e-purse.

ARTs enable monitoring system performance, e.g the velocity of money, and looking for security violations is the purpose of analysing transactions recorded in ARTs after they have been returned in a request for fresh ones. To manage the operations in response to this analysis a DPMI uses the adaptable configurations of both e-vault and its ARTs.

5.3 DPM as a formal money system

The balance of digital money owned by a DPM user is effectively split into two parts: i) a *spendable* part, digitally stored as a number in the e-vault and ii) a *redeemable* part consisting of a number of ARTs stored in the e-purse. The redeemable part of a user balance is the value of any ARTs that has not yet been transferred to the e-vault.

Refinement 2 shows this split balance in a refinement of the model 1. The specification ins refinement 2 are a a formal model for money implemented with ARTs. The two parts of the balance are represented as B and T, respectively for the spendable and redeemable parts. Specification (6) specifies that each user owns the sum of the value of these parts. To make the operational aspects clear the model uses a single ART per user.[31]

The two types of balance tokens in an ART system, e-vaults and ARTs, are represented by B and T,respectively. They both have a value that is positive or zero as shown in specs. (2) and (6).

Specification (8) updates spec. (1) to specifies that all the money in the system is held in these two types of tokens B or and T.

Specification (7) is an updated version of spec. (3). A payment in this refinement involves the payer's e-vault, $\mathsf{B}_{\mathrm{Rob}}$, and the aggregating token of the payee, $\mathsf{T}_{\mathrm{Eve}}$. It shows that in a payment the amount owned by the payer $\mathsf{B}_{\mathrm{Rob}}$ is reduced and the amount owned by the payee $\mathsf{T}_{\mathrm{Eve}}$ is increased.

The *redemption* of the ART for a specific user is indicated by the symbol R presented in spec. (9). It shows that in redemption the value collected in one or more payments with its aggregating token T_u is transferred to the balance B_u. In the redemption the value of the token T_u is set to 0, ready for reuse in receiving one or more future payments for Eve.

The refinement in refinement 2, which introduces two types of balance tokens, in the money system in refinement 2 is clearly compatible with the main system invariant of a constant amount of money in circulation, spec. (1). In refinement 2 money cannot get lost or created during the two specified operations.a˚ß

[31] A model with multiple ARTs is presented in [16]

Refinement 2: Money with an aggregating receipt token

$$\forall u : \mathsf{T}_u \geq 0 \tag{6}$$

$$\mathrm{P}(a, \mathsf{B}_{\mathrm{Rob}}, \mathsf{T}_{\mathrm{Eve}}) =: \text{if } \mathrm{C}(\mathrm{Rob}, a) \wedge \mathrm{A}_{\mathrm{Rob}}(a, \mathrm{Eve}) \Rightarrow \mathsf{B}'_{\mathrm{Rob}} = \mathsf{B}_{\mathrm{Rob}} - a;\ \mathsf{T}'_{\mathrm{Eve}} = \mathsf{T}_{\mathrm{Eve}} + a \tag{7}$$

$$\sum_{\text{users}} \mathsf{B}_u + \sum_{\text{users}} \mathsf{T}_u = M, M > 0 \tag{8}$$

$$\mathrm{R}(\mathsf{B}_u, \mathsf{T}_u) =: \mathsf{B}'_u = \mathsf{B}_u + \mathsf{T}_u; \mathsf{T}'_u = 0 \tag{9}$$

The second refinement, in refinement 3, specifies how the implementation of each of the data modification operations P and R can be atomic and idempotent, which enables a robust, provably correct implementation of DPM.[32]

The refinement specifies three persistent state variables S, T, R to implement the two state variables B and T in refinement 2. It adjusts three operations specified in refinement 2: R , P and C where the new state variables are used. These three state variables have the shared operational constraint that their value is only increasing.[33]

Redemption, spec. (15), is specified as persistently storing a copy T_u in the secure confines of e-vault as $\mathsf{T}^{\dagger}_u$. With $\mathsf{T}^{\dagger}$ the e-vault knows the total aggregate amount of moneys received up to the moment of redemption.

The payment operation, spec. (13), is specified as *incrementing* both values of $\mathsf{S}_{\mathrm{Rob}}$ and $\mathsf{T}_{\mathrm{Eve}}$ by the payment amount a.

With this change, S aggregates the total amount of digital money spend with the e-vault since it's initialisation and T aggregates the total amount of digital money received by its owner.

The payment condition, spec. (14), is modified to first compute the available balance. The available balance is the difference between the aggregated amount spend, S, and the aggregated amount received that has been redeemed, R by the e-vault: $\mathsf{B}_u = \mathsf{R}_u - \mathsf{S}_u$. Both these values have been persistently stored in the e-vault, by the most recent redemption and payment, respectively.

In spec. (12) the computation of the sum of all balances, which is the system invariant for an implementation of money, is modified to match spec. (14) as: $\sum_{\text{users}} \mathsf{T}_u - \sum_{\text{users}} \mathsf{S}_u$. The difference between the two computations is the use of T in the invariant computation versus R in computing the spendable balance. This difference accounts for the gap in knowledge that exists between the e-vault and the outside world, which arises when a payment has been received and not yet redeemed.

With these monotonously increasing values of the three state variables in an e-vault, the consistency of the persistent memory that records transactions in the e-vault can be established as a condition before processing a new one.

An ART is an immutable data structure that moves from a payer to payees accumulating payments. In a payment, a new value is computed for an ART

[32] Storing data atomically guarantees that a write operation writes all data that has been specified as a single unit. This means that the persistent memory is always in a consistent state. A formal model for atomic updates in a secure device is presented in is shown by Butler et al.[6]. This model was based on a patent[15] issued to Jurjen Bos and the author in 2000.

[33] The implementation of a monotonously increasing value requires to further specify a maximum value and additionally allocating a single additional bit to the stored data for each variable. Furthermore, atomicity of an update of such a variable can be realised by replication, at least two, and adding a version counter that is incremented at each update.

from its previous one. The number resulting from this computation, together with any data provided by payee and a hash of the old ART data structure, is then sealed with a digital signature computed with a secret key stored in the payer's e-vault. An ART is an effectively infinitely extendable chain of proofs of receipts of money by the same entity: the e-vault where it can be redeemed.

Redemption is atomically storing the latest extension of the ART, proof of the most recent payment it received, in the e-vault memory.

Extending the value of S recorded in the e-vault persistent memory with a copy of the just computed extension of the payee's ART, T_{Eve}, is the basis for implementing idempotency in a payment.

Refinement 3: Monotonously aggregating balances

$$\forall u : \mathsf{R}_u \geq 0 \tag{10}$$

$$\forall u : \mathsf{S}_u \geq 0 \tag{11}$$

$$\sum_{\text{users}} \mathsf{T}_u - \sum_{\text{users}} \mathsf{S}_u = M, M > 0 \tag{12}$$

$$\mathrm{P}(a, \mathsf{B}_{\text{Rob}}, \mathsf{T}_{\text{Eve}}) =: \text{if } \mathrm{C}(\text{Rob}, a) \wedge \mathrm{A}_{\text{Rob}}(a, \text{Eve}) \Rightarrow \mathsf{S}'_{\text{Rob}} = \mathsf{S}_{\text{Rob}} + a;\ \mathsf{T}'_{\text{Eve}} = \mathsf{T}_{\text{Eve}} + a \tag{13}$$

$$\mathrm{C}(u, a) : \mathsf{R}_u - \mathsf{S}_u \geq a \ '\!\!\rightarrow \{\mathrm{T}\mathit{rue}, \mathrm{F}\mathit{alse}\} \tag{14}$$

$$\mathrm{R}(u) =: \mathsf{R}_u = \mathsf{T}_u - \tag{15}$$

$$\forall u : \mathsf{T}_u \geq \mathsf{R}_u \tag{16}$$

Atomicity in the updates of persistent memory is be realised by replication, as replacement to overwriting the old value, while adding a version counter that is incremented at each update.

In [16] the author proves consistency and correctness of more general version of these specifications.

5.4 DPM versus cash and accounts

Payment with DPM is a digital payment and can be done both offline and online, whereas traditional cash only can be offline.

In addition, in reviewing the four disadvantages of cash presented on page 4 it becomes clear that DPM is better than Plain Old Cash: i) DPM cannot be stolen, the e-vault requires owner authorisation and an ART can only be redeemed at the payee's e-vault (item a)); ii) The physical size of digital information is determined by the size of the computer that stores it in its memory. The amount of information to store records of payment transactions is in any present-day computer effectively unbound.[34] (item b)); iii) The proof of payment token computed as result of processing the payment acts as a receipt. It includes a reference to the payee and the amount anf any data provided by the payee for inclusion in the receipt. (item c)) and iv) ART technology DPM can support AML in a more effective manner, so it is less suitable for laundering money (item d)).

As a distributed peer-to-peer system of devices that implements peer-to-peer payments, DPMI provides: i) no operational costs to make a payment;

[34] As mentioned above, the enhanced physical security of an e-vault intended for larger amounts can require more bulk and weight. Such an e-vault would still be much smaller than the corresponding amount of cash.

ii) zero latency in in–person payments; iii) low latency in online payments; iv) no constraints to scalability and v) capability to operate without data communication networks. No digital payment system using a ledger and intermediated updates to account records can provide these features.

6 Conclusion and future work

A Digital Public–Money Infrastructure could be the future foundation of the monetary system fit for a digital world. It provides a robust, secure implementation of universally available digital money that can be operated tightly integrated in the existing monetary infrastructure. It offers existing players the use of low–cost direct instantaneous settlement in any amount over any distance.

Through the DPMI all participants in the economy, citizens, merchants, SMEs, large corporations, financial institutions and government agencies, all alike, can own and use digital public money. Parties can make their payments directly to strongly authenticated payees, in any amount, over any distance with instantaneous finality. Digital public money is cash that is better than Plain Old Cash.

Consisting of many e-vaults under direct control of their users, the DPMI is a highly resilient, robust distributed system that offers effectively unbound transaction capacity. Not requiring centralised transaction processing the DPMI reduces the cost to society for the use of money. It increases overall system security.

A formal model for the implementation of digital money based on ART technology demonstrates with mathematical rigor the feasibility of DPM as a distributed implementation with managed security. The elaboration of this formal model elsewhere ([16]) provides mathematical proofs for claims that the system strongly protects the monetary value stored and paid.

Future work could elaborate on each of the uses cases presented in section 3.3, either separate or combined e.g financial focussed on central banks, commercial banks, other financial institutions, businesses focused on merchants and SMEs, and consumers as individuals and households. Investigating the monetary aspects of instant finality of direct, sub-second payments could also be a topic. The impact on liquidity management in SME payments from the immediacy enabled by direct payments in DPM and its effect on the wider economy would be interesting to learn.

As DPMI King Cash returns, restored to full strength clad in a new, shiny, tamper-detecting armour, wielding an invisible aggregating token to bring wealth to all.

Bibliography

[1] Michel Aggietta et al. *La monnaie souveraine*. Odile Jacob, 1998. ISBN: 9782738106315.

[2] Ulrich Bindseil, Fabio Panetta and Ignacio Terol. 'Central Bank Digital Currency: functional scope, pricing and controls'. In: *Occasional Paper Series*. 286. European Central Bank, Dec. 2021. URL: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op286~9d472374ea.en.pdf.

[3] BIS task force on security of electronic money. 'Security of electronic money'. In: Report 1. Report produced by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries. Basle: Bank Iinternational Settlements, 1996, p. 64. ISBN: 92-9131-119-7. URL: https://www.bis.org/cpmi/publ/d18.htm.

[4] Finn Brunton. *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*. Princeton University Press, 2019. ISBN: 9780691179490. URL: http://www.jstor.org/stable/j.ctvc77f9r (visited on 21/05/2022).

[5] Michael Butler and Divakar Yadav. 'An incremental development of the Mondex system in Event-B'. In: *Formal Aspects of Computing* 20.1 (2008), pp. 61–77. ISSN: 1433-299X. DOI: 10.1007/s00165-007-0061-4. URL: https://doi.org/10.1007/s00165-007-0061-4.

[6] Michael Butler et al. 'Transacted Memory for Smart Cards'. In: *FME 2001, Formal Methods for Increasing Software Productivity (01/03/01)*. Ed. by J. N. Oliveira and P. Zave. Address: Berlin. Mar. 2001, pp. 478–99. URL: https://eprints.soton.ac.uk/253695/.

[7] *Central bank digital currency: opportunities, challenges and design*. Tech. rep. 4. Bank of England, Oct. 2020. URL: https://www.bankofengland.co.uk/paper/2020/central- bank-digital-currency-opportunities-challenges-and-design-discussion-paper.

[8] David Chaum. 'Blind Signatures for Untraceable Payments'. In: *Advances in Cryptology: Proceedings of CRYPTO '82*. Plenum, 1982, pp. 199–203.

[9] *Electronic money system security objectives*. Tech. rep. Based on common criteria. European Central Bank, May 2003. eprint: ISBN92-9181-362-1.

[10] 'Exploring anonymity in central bank digital currencies'. In: vol. 4. In focus. European Central Bank, 2019. URL: https://www.bis.org/cpmi/publ/d18.htm.

[11] M.G. Gouda and A.X. Liu. 'Formal specification and verification of a micropayment protocol'. In: *Proceedings. 13th International Conference on Computer Communications and Networks (IEEE Cat. No.04EX969)*. Oct. 2004, pp. 489–494. DOI: 10.1109/ICCCN.2004.1401715. URL: https://ieeexplore.ieee.org/document/1401715.

[12] Gesine Hinterwa¨lder et al. 'Efficient E-Cash in Practice: NFC-Based Payments for Public Transportation Systems'. In: *Privacy Enhancing Technologies*. Ed. by Emiliano De Cristofaro and Matthew Wright. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 40–59. ISBN: 978-3-642-39077-7.

[13] Shunsuke Inenaga, Kenichiro Oyama and Hiroto Yasuura. 'Towards Modeling Stored-value Electronic Money Systems'. In: *IPSJ Online Transactions* 3 (2010), pp. 176–185. DOI: 10.2197/ipsjtrans.3.176.

[14] Innovation hub experts. 'A high–level design guide for offline payments with CBDC'. In: Project Polaris part 4. Bank International Settlements, Oct. 2023. ISBN: ISBN 978-92-9259-701-6.

[15] Eduard de Jong and Jurjen Bos. *Arrangement storing different versions of a set of data in separate memory areas and method for updating a set of data in a memory*. EN. Pat. Dec. 2000. URL: https://www.freepatentsonline.com/6769053.html.

[16] Eduard Karel de Jong. 'A formal model of money as foundation for a Digital Public Money Infrastructure'. Unpublished. Jan. 2026.

[17] Eduard Karel de Jong. *Digital asset markets with offline public money*. Working paper 1. University of Manchester, 2025. URL: https://documents.manchester.ac.uk/display.aspx?DocID=76930.

[18] Jerome H. Saltzer and Micheale D. Schroeder. 'The protection of information in computer systems'. In: *CACM* 17.7 (July 1974). URL: %5CURL%7Bhttps://www.cs.virginia.edu/~evans/cs551/saltzer/%7D.

[19] Leo Van Hove. 'Electronic purses: Which way to go?' In: *First Monday* 5.7 (July 2005). DOI: 10.5210/fm.v5i7.770. URL: https://journals.uic.edu/ojs/index.php/fm/article/view/770.

[20] Joseph B. Walton. *Why we use a new currency: the role of trust and control in explaining the perception and usage of Bitcoin*. PhD. 2020.

[21] T. H. White. *Arthur: The once and future king*. Collins, 1958.

[22] Wikipedia contributors. *Mondex — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Mondex&oldid=1306224924. [Online; accessed 19-September-2025]. 2025.

[23] Alejandro Zamora–Pe´rez, Eliana Coschignana and lorena Barreiro. 'Ensuring adoption of central bank digital currencies – an easy task or Gordian knot?' In: Occasional paper series 307. European Central bank, Oct. 2022. URL: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op307~c85ee17bc5.en.pdf.