How the King returns:  
A digital future of cash

Eduard de Jong

22nd May 2023

(version 1RC5)
Pre-publication—for review

Abstract

Over the last ¾ century society has become largely digitised. Banks were early movers digitising their ledgers as databases. Cash, banknotes and coins, up till the present could not be digitised. This paper shows how cash can be digital, as e-cash. E-cash is a form of money with all the features of traditional cash that brings additional benefits from being digital. Digital e-cash can be paid from person to person or over the Internet, it can be withdrawn from a bank account without visiting a physical ATM and deposited as easily. By nature e-cash is a distributed IT system with a large number of secure personal digital devices, electronic purses (e-purses), that can pay purse to purse with finality, without intermediation, protecting payer privacy and without per-transaction fees. With a presented information model of money as guide and applying aggregating token technology to secure the transfer of value, the implementation of this system can be based on a high level architecture consisting of just three basic functional components: i) an electronic purse as a digital bearer payment instrument to store, pay and receive e-cash, ii) an issuer of e-cash and guarantor of the system security and iii) an agent to support users and gather management information. This paper demonstrates how users of the e-cash system, citizens, merchants, the issuer and financial institutions can each benefit from participating in the digital future of cash realised with an adaptably secure e-purse and its supporting services.

Keywords: cash, digital money, e-cash, electronic cash.

1 Introduction

Over the past three decades in many parts of the world remote electronic transactions have steadily replaced the use of coins and banknotes as the way to pay. The extend to which cash is being replaced as a means of payment differs greatly over the world and within countries. Several segments of the population continue to rely on physical cash. E-cash might be an instrument to make digital payments accessible to these people.
result of this digitalisation of money. The figures shows that digitisation has been realised for two of the three well known types of money in a monetary system.

Cash with its foundation in handling physical object like coins and banknotes, has been difficult to digitise; only bulk handling of cash, in particular cash counting, has been automated. The digitisation of commercial bank money enabled to replace payments with cash by electronic payment using secure technology like PIN&Chip\(^2\) in banking cards. Online communication via secure payment terminals make payments to merchants digital by remotely updating centralised databases with user accounts. Digital payments to non-merchants is much more recent development that leverages the ubiquity of smart mobile phones to provide the required hardware security.

Since about 2015 discussions have emerged on how to achieve a digital currency issued by a central bank, CBDC, for “Central Bank Digital Currency”. These discussions revealed that current digital payment solutions, with accounts, cards and the web, are deficient in a fundamental way: These payment methods lack essential propertries of cash. Cash is accessible to all, its payments are anonymous, immediate, and final. A cash payment is between two parties, without intermediaries of any kind. It does not requie fees.

Hence, in order to fill that gap, a generally acknowledged requirement for CBDC is that it must be “cash-like”. The challenge in filling the hole in the table in fig. 1 to implement CBDC is to apply a digital technology that is the most like cash. A digital technology for payments that are offline, for securely storing digital currency detached from a centralised account so that it can be adopted by many people for a range of daily payments. Just like cash.

In English there is a saying, “Cash is King”. Cash puts a buyer in the strongest position. Any purchase can be completed immediately and without question. There are no delays, dependencies, or intermediaries. Accepting cash is an easy decision for the seller.

In the Arthurian legend, without the king, Arthur, on the throne, dark forces clouded the future. In analogy, in our times King cash is absent in the digital realm excluding parts of society from the larger financial system.

When King Arthur returned and pulled the sword from the stone, he ushered in an era of peace and prosperity, much as cash did for commerce.

\(^2\)PIN&chip refers to the use of a smartcard as banking card with the chip locally validating the user.
scores of centuries ago. While the existing payment products are suitable in some situations, the lack of a digital cash option limits commerce in multiple ways.

Let us then digitally increase prosperity with the return of Cash, the King.

This paper presents e-cash technology to concretely realise a digital equivalent of cash based on the technology proposed by the author in [4]. This secure e-cash technology allows King Cash to pull his metaphorical sword from the stone where it is presently stuck. With this technology the King can return to its place on the throne, bringing back money as a widely accessible public good, as digital e-cash.

The paper is organised as follows: The next section presents an information model as basis for the design of digital money and demonstrates its suitability by analysing existing types of money. Section 2 presents an overview of the system architecture to implement transferrable e-cash as a new, digital, type of money, highlighting the central role of the e-purse, the secure container of digital currency. Section 4 zooms in on the functional architecture of the e-purse showing details how the security can be realised in the device and during a payment. Section 5 describes the central functions performed by the issuer as the responsible identity for the correct and safe operation of the whole money system. Section 6 describes the e-cash handling operations in financial institutions to support withdrawing and depositing e-cash. A conclusion and bibliography completes the paper.

2 Types of money

To develop an Information Technology IT system to implement the digital equivalent of cash an information model of money is an essential aid. Such a model identifies the information being processed and the critical operations performed in the system by its users that lets them experience it as money. In [4] the author presented a model for money as information using a mathematical formalism. This model can be summarised as “Money is a number with an owner,” with the owner deciding when that number can be changed by making, or receiving, a “payment.”

Model 1 formally presents the model that is based on the following seven components: \{U, B, \omega, \mathcal{P}, \alpha, I, E\}.

---

3The presented model is an enhanced version of the model presented in the reference; it has further details on the money issuance process.
The symbols in the model that represent the components in the model have the following meaning: $U$ is the set of all users, each the potential owner of money; $B$ is a set of balances $B \in \mathbb{N}$, numbers that each represent a specific amount of money that can only be changed by its owner in accordance with the rules in the model; $\omega : B \rightarrow U$ is the ownership association between a balance and its owning user; $\mathcal{P} : B \times \mathbb{N} \times B \rightarrow B \times B$ is the payment operation in which a pair of balances is modified with an amount $a \in \mathbb{N}$ applied in opposite directions; $A : U \times \mathbb{N} \times U \rightarrow \{\text{true}, \text{false}\}$ is an authorisation given by the first user, Rob $\in U$, the payer, to make a payment of an amount $a \in \mathbb{N}$ to the second user, Eve $\in U$, the payee$^4$; $I \subset U$ is the set of users that can act as issuer and $E$ is the set of issuing events $e_{ij} \in \mathbb{Z}$, which are the amounts of money being issued or, if negative, withdrawn, at time $\tau_j$ by issuer $i$.

The ownership relation $\omega$ is represented in the model by writing the balance for owner $u$ as $B_u$, it is not used explicitly. That the money issuing events are ordered in time is stated in formula 1, which restriction is needed to make the next two formulas logically consistent. Formula 2 shows that at a specific point in time $\tau_j$ the balance of the issuer $i$ for that event is increased by an amount $e_{ij}$ at that point in time, as stated in formula 3, the total amount of money in the system increases by the same amount. Formula 3 is a system constraint stating that the total amount of money is constant for the episode between two issuing events. This constraint is a key system property; it means money cannot disappear or emerge out of thin air, except in an issuing event. In this model the payment authorisation function is written as $A_{\text{Rob}}(a, \text{Eve})$, using the subscript Rob as way to indicate that the details of how a user gives its authorisation can be fully defined by each payer while the payee and amount are parameters in the computation of the result. Authorisation $A$ is used in formula 4 as a condition for making the payment.

The key features in this information model of money are that i) there is only one operation, payment ($\mathcal{P}$), that can modify the value of a balance for every user; ii) the total amount of money in all balances is a constant value; iii) payment modifies a pair of balances in tandem by the same amount; iv) a payment can only be made if approved by the owner; v) an issuing event changes the total amount by changing the balance of a single issuer and vi) except for the issuer affected by an issuing event, no user is aware of the change of the total amount.

$^4$Payment to its own balance need not be excluded from the model so Eve can be the same user as Rob.
That the owner of money controls spending is a property that is rarely made very explicit but it is essential: The decision by a user to make a payment is a decision on the subjective value represented by the amount by which the payer is willing to reduce the balance\(^5\); it is what makes the balance information to be experienced as money.

The payment operation is an atomic, pairwise update in opposite direction of two balances that clearly fulfils the system constraints in 3: the amount of money in the system before and after the operation is the same. The fulfilment of the system constraint is independent of the total amount of money, as it only involves two parties Eve and Rob and their respective balances \(B_{\text{Eve}}\) and \(B_{\text{Rob}}\). The value of \(B\) is persistent and the only way it can be changed is either in a payment operation or in an issuing event.\(^6\)

The information model of money describes cash, as will be elaborated below.

Commercial bank money, in the middle column of fig. 1, is another type of money that implements this information model. In this type of money the balances are recorded in a central database, a digital ledger\(^7\), maintained by each bank. The implementation of ownership \(\omega\) needs a database to record personal data used to authenticate a user’s payment instruction. The banks also act as issuers.\(^8\)

In contrast to cash, commercial bank money is a centralised implementation of money. A payment is intermediated by the payer’s bank. All payments are processed by the same computers and each one is recorded in the ledgers managed by these computers.

Cash as information

In cash ownership \(\omega\) is ‘implemented’ by a physical container under control of the user, that holds the objects that represent the monetary value. The coins and banknotes encode the value of a balance in multiple digits in a mixed radix representation\(^9\) in which each digit has a different radix, each corresponding with one of the available different currency denominations of banknotes and coins. Each digit in this representation in its turn is represent-

\(^5\)The model shows how the two properties of money identified by economists, as a means of payment and as a store of value in an information perspective are really intertwined: A secure store of value is essential to having exclusive control on when to spend, how much and to whom. In that way it is the psychological precondition for both making and receiving a payment. Observations in the field of user perceptions on different methods of payment reported by Narula et al.[10, pp. 20–21] confirm how important this control is for users. To use a fitting metaphor, these two functions of money are the sides of one and the same coin.

\(^6\)To realise the persistency and constraint on mutability of the balance \(B\) is a technical challenge. A secure IT device, cryptography and software that have been proven as correct is needed to meet that challenge. These parts of the solution are mature technologies and are readily available.

\(^7\)A digital ledger is a database that implements specific rules, e.g. applicable to payment (see formula 4), for updating records.

\(^8\)C.f. [11], a report by the Deutsche Bundesbank that summarises the different issuing events where this type of money is created and destroyed.

\(^9\)Computer scientist Donald Knuth describes mixed radix representation of numbers in [7]
ted by an unary encoding: By counting objects that are immutably marked with the radix value. The value of the balance $B$ is tamper resistant by the protection offered by the owner’s physical container and it is unmodifiable by the way a banknote or coin is manufactured. Payment is authorised by payer Rob by removing coins and banknotes representing the amount to pay $a$ from the owner’s container, which implements $B_{Rob}' = B_{Rob} - a$ in formula 4. Payment is completed by payee Eve receiving the objects removed by Rob from his container (purse) and adding these to her container (purse) implementing $B_{Eve}' = B_{Eve} + a$ in that formula.

In the Eurosystem there are multiple issuers of cash, the national banks of its member states, while the European central bank coordinates the issuing events; in the US the Treasury department is the single issuer of cash.

Cash is fully decentralised implementation of money. Information storage and processing is done by each owner when taking money objects out, or putting them in, their private container. Each amount is ‘computed’ locally by both payer and payee by counting objects. Because of the required counting, ‘computing’ a payment in cash requires effort and time from both parties.

The information model of money shows that an implementation of e-cash must also be decentralised. The remainder of this paper shows how that can be done.

Money in a monetary system

Bitcoin and many other claimed digital currencies can also be described by the information model of money presented above. As 15 years of experience with such “crypto currencies” shows, it is not enough for a system that implements the information model of money to be actually usable as such. What is needed is the embedding in a monetary system (c.f. fig. 1). The monetary system provides an anchor for the monetary value of all types of money it includes, allowing these different types to be used interchangeably in a range of payments.

Cash issued by a country’s central bank provides that anchor. As the anchor, cash sets the unit of account used in all types of money in a monetary system, that unit is defined as one of the denominations of the issued cash ‘objects’. The digital form of cash, e-cash, also issued by a central bank, fits right in. It will add strength to that anchor.

---

10Milner [9] makes the point that bitcoin is a centralised implementation of money with transactions recorded in a shared database. The transaction database is replicated over the processing nodes that form a peer-to-peer network. Due to the intricacies of correctly implementing transaction handling in a distributed database, a balance is represented as a collection of immutable fragments. In a payment operation an update of the balance of a payer marks one or more fragments as no longer valid as they have been ‘spend’. The result of a payment is a new balance fragment recorded for the payee and, possibly, one additional balance fragment recorded for the payer if the amount of the spend fragments exceeds the payment amount. Adherents of bitcoin refer to these recorded fragments as “coins” that they call “UTXO”. Garret et.al[3] confirm the centralised nature of bitcoin while acknowledging the possible perception of balance record fragments as “tokens” or “coins”.

©2023 de Jong Inventions I BV

6
3 A digital type of cash: e-cash

A payment in e-cash involves only two parties, the transfer of value is finalised there and then, there are no per transaction costs. A payment in e-cash can be from person to person, from consumer to a merchant, from merchant to supplier, from business to business, from citizens and corporations to government and from governments to all. Like cash, e-cash payments are A2A, anyone-to-anyone.

Figure 4 shows the design of an IT system to implement e-cash based on the information model presented in the previous section. In analogy with traditional cash, this design of e-cash is also decentralised, with digital information being stored and processed locally. The e-cash system has three operational components:

- The e-purse, an IT device used by all users to store e-cash that implements the payment operation $P$ and the payment authorisation function $A$;
- The issuer, an IT system dedicated to maintain security of operations of the system operations that includes a specially configured e-purse to implement issuing money;
- The supporting agents, one or more IT systems that support the continued operations of e-purses implementing the security policies and monetary controls set by the issuer.

The issuer and e-purse components reflect the information model for money, with a balance held by each user and by the issuer, respectively. The operating agents in fig. 4 are a design artefact reflecting the implementations of operational requirements for an IT system to securely implement e-cash like the ability to monitor and control its operations, and its interface with IT systems that handle other types of money in the monetary system.

With these three components e-cash can be implemented as a new type of money, which can be used very much in the same way as Plain Old Cash. In particular this e-cash protects payer privacy as a payee cannot get any information about the payer from the money that it receives.

With digital money stored in an IT device, the e-purse, a user can experience handling e-cash much like handling cash as both involve handling a physical object. E-cash is actually better than cash: An e-cash payment i) is effortless for any amount by its electronic computations; ii) is fast by digital communication; iii) can also be made online and iv) immediately provides the payer with a cryptographic proof of payment. E-cash can’t be stolen.

11The IT architecture figures in this paper use a modified UML notation for functional components in an IT system. The diagrams show a component composed of sub components that provide services to each other and the outside.

12The e-purse is locked by a PIN or fingerprint or a combination for payments over a certain, configurable amount and stealing an e-purse gives very little gain to the thief, if any. E-cash received in payment is digital data that is cryptographically bound to the intended payee and
the size to store it does not grow proportional to the amount, and receipts of payments can be analysed, pseudonymously and retroactively, by the issuer or an agent for AML violations. E-cash complements Plain Old Cash and delivers convenience, privacy protection and operational costs at a level better than card payments and online banking can.

The e-purse is the only component in this e-cash system that is involved in handling money, it is the only functional part equipped to securely make and receive payments. Figure 4 shows this with the payment operation as a green line between the payee and payer functions of an e-purse. Its key functions are to: i) initiate a payment by sending a request to a payer, ii) approve payment of a specific amount to a specific payee, iii) make payment in response to an approved payment request, iv) present the balance of funds available, v) interact with supporting agents to support security and monetary controls, vi) be initialised with an amount of e-cash, vii) detect physical abuse in order to respond to attacks by disabling its operation and saving the amount stored for later recovery, and viii) recover funds once terminated.

As an IT component the number of functions of an e-purse is small. The size of the software to implement these is also small, small enough to create the software in a rigorous manner, using formal methods and security-aware software engineering. This development process combined with extensive security testing will assure that the e-purse software has no bugs. The processing components needed to construct a highly secure e-purse are readily available. It can be built to a security level that fits with deployments to hundreds of million of devices. Section 4 presents further details of the construction of an e-purse.

An e-purse is the digital equivalent of a bearer payment instrument. Like the role of a banknote in a payment in Plain Old Cash with its clearly recognisable intricate printing, an e-purse conveys by its design and operation a security guarantee from the issuer to both parties involved in a payment. A user obtains the e-purse already laded with e-cash with money obtained from the issuer; the diagram in fig. 4 shows this as connection between the issuer and special initial loading function. Provisioning an e-purse to its user can be done by commercial banks, for their banking customers, by social services or by post offices. The latter agent supports users that have no bank account.

In an e-cash system the issuer issues e-cash, makes e-purses available for provisioning of users and manages the operations and security of the system. There exist only one issuer in the system. Section 5 presents details of the core functions of the issuer.

The third operation component in the e-cash system is a collection of operating agents, which provide a number of services to the issuer and users to keep the system running smoothly and securely. They interact regularly with the e-purses to refresh stored information needed to make payments: To validate a payment the e-purse uses a number of cryptographic keys, to request a payment the e-purse uses aggregating tokens, both secret keys and aggregating tokens have an expiry date. The regular refreshing of these

---

13The trusted supply chain to securely provision e-purses is available from various suppliers, e.g. those of smartcards.
14An aggregating token is cryptographically protected message that allows a payee to se-
data elements in an e-purse enables updates of the system configuration in each of the deployed e-purses.

One type of operating agent is dedicated to the first interaction with an e-purse at the point where it is handed over to a user in order to initialise it for use by a specific user. During initialisation the e-purse is loaded with its initial value in e-cash from a dedicated e-purse provided to the operating agent by the issuer. Providing an e-purse to users can be done in different ways adapted to the local circumstances of each potential user.

The various functions provided by operating agents are accessible online and can be implemented by a single operator, for instance a bank, or by multiple independent service providers such as social services or the post office. Operating agents do not handle e-cash, their role is to maintain system operations and security. The issuer vets operators and sets quality requirements for the security equipment they need.

Figure 5 represents the result of deploying e-purses to private and commercial users. It shows an e-cash system with a number of private users, in yellow, and a merchant, in green. The users can make payments to each other and to the merchant; the merchant and some of the users can make deposits and withdrawals to/from their bank accounts. Deposits and withdrawals are made as e-cash payments to and from an e-purse operated by the bank.

Some users don’t have bank accounts and receive e-cash from other users, e.g. employers or social services. A payment can be sent to a recipient as a QR code and an unbanked user can visit a website and scan a code to receive money. With aggregating token technology money send as payment to a user cannot be stolen; a QR code for a payment can safely be displayed on a webpage, that could be read, for instance, at a library.

Liquidity in the system is supported by banks. They can arrange with the issuer to withdraw or deposit e-cash with the issuing central bank against their reserves. They could also have arrangements with other banks to make or receive or provide e-cash funds. Liquidity management is fully digital and instantaneous.

---

©2023 de Jong Inventions I BV
4 The e-purse as bearer payment instrument

An e-cash system is a large collection of interacting e-purses. Most e-purses are owned by citizens; many e-purses can be owned by merchants and other small and medium size business. Figure 5 shows how banks, post offices, and social services play a role in distributing e-cash. With an e-purse all these different users can pay and receive e-cash to and from each other.

Figure 6 shows the functional components in the implementation of an e-purse. The core component in an e-purse is the MonEbox, a dedicated security module that holds a balance of e-cash. It also contains the secret cryptographic keys to make a valid payment and the executable code that implements the secure payment protocol. The MonEbox is built to protect itself against tampering, erasing the secret keys and saving the balance when an attempt to abuse the device is detected.

The level of physical security provided by the MonEbox is higher than can be obtained with traditional smartcards alone,\(^{15}\) this higher level is required to make the MonEbox a strong security foundation for a distributed system that consists of hundreds of millions of e-purses that each store money issued by a central bank. Upon this foundation security can be actively managed by monitoring and adjusting operational configurations in response to observed behavior. A 1996 BIS report\(^{2}\) on e-cash security provides a baseline for this configuration. More recently, with Cattaneo the author has presented\(^{6}\) an outline for fine grained run-time adjustable configurations to differentiate between various use cases based on their different risk profiles.

The user interface component enables the user to control the e-purse, to see its balance, to initiate a payment and to approve making one. An e-purse can be built with each of these two components as a distinct device. For instance, the user interface can be implemented as an app on mobile phone and the MonEbox as a separate, dedicated, personal small device, like a key-fob. The mobile phone app communicates with its own MonEbox via BlueTooth (BLE). To receive a payment the phone app can communicate with another e-purse via NFC, QR codes or via the internet.

The e-purse phone app can offer additional functions, for instance to review payments received or made in a particular period or to budget future spending. Budgeting cash outflows is a function much appreciated by users that mainly pay in cash as described by Mas\(^{8}\). The app can schedule recurring payments, or payments to made once sufficient balance is available. It can be separate or part of a more comprehensive wallet app or a point-of-sale app.

\(^{15}\)A smartcard is characterised as “tamper resistant”, the MonEbox is “tamper detecting.” Tamper detection has the double effect of a major increase in the effort, time and money needed to penetrate the device, and in effectively eliminating the value obtainable by penetrating.
The MonEbox is a digital bearer payment instrument; just like a banknote it is manufactured and provisioned to the user under control of the issuer. A MonEbox has a display to show its balance and a button to push as physical means of approval for a payment. The MonEbox is configured at issuance for the minimum amount that needs approval with a button press to constrain the damage that can be done by rogue software that could penetrate the user device, e.g. Pegasus. The user can set a lower approval limit. A MonEbox can support interface devices for multiple users or by the same user on multiple devices. With multiple users the security of access by each of them is configured at device issuance.\(^\text{16}\)

The e-cash system uses aggregating tokens\(^\text{17}\) to request and receive a payment. An aggregating token is secure message that cryptographically binds an amount of e-cash to its owner, which means that the MonEbox is not needed to initiate and receive a payment. This can be done by the user-interface device. Merchants with multiple points of sale can install a single e-purse in an office computer to provision aggregating tokens. Webshops have many points of interaction in the cloud instances of their webserver, the cloud instances can be provided with aggregating token’s from a dedicated server that includes one or more e-purses.

Figure 7 shows an e-purse integrated in an IT system where it uses the systems internal data network, WiFi or Ethernet, to communicate with users. The users use a e-purse user interface app or a webbrowser to interact with the e-purse. This e-purse provides two functional components: i) to handle requests from users to ask a customer for payment, for instance to create a QR code to present on a web page or show in the pdf of an invoice; ii) to manage the outflow of e-cash in accordance with corporate governance practices. The first function also involves managing the aggregating tokens, assuring there are enough to handle an expected number of payments. The second function relies on the configurability of the MonEbox. The MonEbox can recognized multiple users, which can be configured in single or joined signature schemes with different spending levels. These user can be securely identified by secret cryptographic keys stored in a mobile phone app or a commercially available hardware authenticator.

Figure 8 shows the functional structure of a MonEbox: i) a smartcard that implements the core security operations, storing secret cryptographic keys, the balance of e-cash, and the program code that implements the payment functions and ii) a processor that implements the communication with the user interface device(s), handles the display and button, monitors tamper detection sensors, responds to tampering and manages the battery.

\(^{16}\)For a MonEbox in a corporate setting, the user configuration can be adjusted later, e.g. by the CFO. A special configuration app will be available for that purpose, which uses NFC to securely do this. (See also fig. 7)

\(^{17}\)An aggregating token is generated for a particular user by one of the operating agents. See [4] for more details
The smartcard can be one of the widely available high security chips based on Java Card technology. As a Java Card chip it supports implementation of the different security functions as separate applets, which can be updated with the latest software at the time the MonEbox is issued to its user. Updating configurable data in the smartcard can, for security reasons, only be done through its NFC interface. The NFC interface can also be used for low value payments, which can be made irrespective of the state of the battery.

Handing a MonEbox to a user includes setting up the security of the communication with the user’s phone or tablet. In addition to pairing the Bluetooth connection, the phone stores a freshly generated communication protection key shared with the MonEbox. The communication keys can safely be stored in the secure enclave or trusted execution environment (TEE) that is offered by most mobile phones.

A MonEbox can be built in different forms to accommodate use cases that differ in the number of users and the amounts that can be paid with or stored in the device:

i) for an individual user, and ii) for a family or a small business where a few users could each make payments, and each user has its own phone or tablet and iii) corporations like banks where larger amount of money is stored and multiple users may authorise payments either alone or jointly and iv) machines that pay other machines for IT services they may need from time to time.

An e-purse for use by a business is functionally the same as a user one, however, its user interface component is a software module implemented in its IT system. The user interface software communicates with the MonEbox to request and authorise a payment. The MonEbox for a corporate e-purse may be built as a device that meets higher physical security requirements to reflect the larger monetary value it stores and can pay.

5 Issuer

Figure 9 shows the functional components of the implementation of an e-cash issuer in the context of the issuer’s IT system. The issuer provides the liquidity for e-cash users with its issuance component that incorporates
the issuer’s e-purse, with which it can receive or send e-cash from or to financial institutions and to user e-purses being initialised. The issuer e-purse is specially constructed as an air-gapped hardware security module (HSM) that implements issuing events. An issuing event requires an instruction from a qualified number of specially configured in the e-purse as issuing operators. The figure shows these operators as an issuance committee.

The issuer e-purse further operates like any other bank’s e-cash component in interaction with the financial administrative system to support withdrawals and deposits by the issuer’s e-cash using customers like banks. This is discussed in the next section and shown in fig. 10.

The issuer realises its management of system operations and supervision of its security through the operational agents shown in fig. 4. These issuer function are implemented with components dedicated for managing e-purses and e-cash, and to adjust operational configurations. Those operating agents that receive e-cash from the issuer, or make deposits, can do so with the support implemented by a dedicated functional component that includes a Mon\textregistered{} box.

6 E-cash and financial institutions

Financial institutions play the same role in e-cash as in Plain Old Cash, except all operations and interactions being digital.

Figure 10 shows the functional component integrated in a bank’s IT infrastructure to implement withdrawals and deposits in e-cash. It shows the bank’s e-purse\textsuperscript{18} and the two software components implementing these two e-cash operations. These implementing components are shown to receive requests from a user via a webserver implementing a standardised e-cash API, which can be integrated in the bank’s banking API servers. The bank’s IT infrastructure also contains a token factory that can be used to create the special aggregating tokens used by both the bank and the user to secure the deposit and withdrawal, respectively.

Figure 10 also shows functional components in the banks IT system with which the e-cash component interacts. The customer account system is needed to record the withdrawal and deposit operations as debit and credit mutations, respectively. The banks

\textsuperscript{18}In practice this e-purse will be implemented with multiple Mon\textregistered{} boxes, in particular a single one to receive payments as the identified owner of the received e-cash. Another Mon\textregistered{} box can be used for withdrawals and deposits with the issuer’s e-purse. To make payments to users to effect a withdrawal, a number of Mon\textregistered{} boxes can be deployed to realise an acceptable latency for withdrawals.
webserver has to implement the web API to handle requests from customers to be forwarded to the withdrawal and deposit components.

The bank’s token factory, and the identifier provisioning component, both marked in blue, are generic operating agent components in the e-cash system. They offer their e-cash support services to bank customers for use by the customer e-purses. The bank customer data base is used as the authoritative source of the identity information needed to initialise an e-purse at issuance to a customer. It also provides the bank account number to be included in the depositing token. These operating agent components communicate with the issuer for monitoring and control.

The user can initiate an e-cash deposit with the e-purse user interface by making a payment to the bank. The bank uses an aggregating token for its e-purse that is specially created for a specific customer by including the bank account number. Receiving a deposit payment with such a deposit aggregating token will lead to a credit to the customer's account by the implementation of the deposit component.

The deposit aggregating token is stored in the user’s user interface device and can be reused for a number of deposits. The user’s user interface could be programmed to make a deposit automatically, e.g. for a merchant to deposit the daily receipts.

The e-purse user interface is also used to initiate a withdrawal of e-cash from a bank account. The withdrawal is done as a payment request send to the bank’s online server. A payment in e-cash is then made from the bank’s e-purse after the withdrawal component determines that the user has sufficient funds. The withdrawal payment uses a specially constructed aggregating token that includes the public key corresponding with a user’s cryptographic withdrawal authorisation key. As a withdrawal is a payment to the user itself AML checks are not needed.

This use of aggregating token technology shows how e-cash can seamlessly interface to online banking by adding extra, dedicated data to some of the tokens.

The e-cash balance maintenance component interacts with e-purses operated by other banks and the issuer to manage the liquidity in e-cash. This component executes the liquidity management decisions by making and receiving e-cash payments. These payments use aggregating tokens obtained from issuer’s agent operation support component (c.f. fig. 9). In the messages exchanged between the banks for these payments in the standard MT940 format, an aggregating token corresponding to the account mutation specified can be included in a field added to that standard.

The implementation of the balance maintenance component can use parts of the implementation of the withdrawal and deposit components, e.g. the interface with the MonEbox. This specific component is also part of the implementation of the issuer’s issuance component (c.f. fig. 9).

\[^{19}\text{The withdrawal key can securely stored in the MonEbox, its use is illustrated by Auer en Böhme[1, p. 94] as token access to a CBDC bank account.}\]
7  Conclusion

The technology exists to issue a new, digital type of money that complements the three traditional types of money: cash, commercial bank money and bank reserves. This new type of money is electronic cash, e-cash; its circulation is based on a digital bearer instrument in the hand of a user, the e-purse, which can receive money from any other e-purse. The e-cash in circulation is created by a dedicated secure device operated by the issuer.

A payment in e-cash is directly between two parties, settles immediately and without intermediation, does not have costs and hence no fees, and it can be made face to face or over a distance, e.g. for a web purchase or remittance.

The e-purse can use an app on a mobile phone or tablet or a program on a business IT system to providing a rich, programmable user interface. For specific use cases it can also be a smart card with a display and some buttons. The e-cash storing security module, the MonEbox that is an integral component of an e-purse is a digital bearer payment instrument. The MonEbox in an appropriately strong physically secure form, is also the e-cash handling payment component in banks and other enterprises.

E-cash is money usable in any digital environment both offline and online. A payment in e-cash does not need the use of a communication network, it does not need an identity register for authentication and authorisation, it does not need a transaction database to finalise the value transfer. This innovation in money will be disruptive for incumbents with business models based on the revenues of intermediated payments.

E-cash will also disrupt the business models of money launderers and tax evaders as the system provides income transparency, a pseudonymous, undeniable, secure digital record of all digital income.

8  Bibliography


