Digital Asset Markets with Offline Digital Public Money

Eduard de Jong

21st July 2025 (version 2)

Abstract

As an offline, digital representation of ownership of a (digital) asset, a digital asset token (DAT) is data stored in a computer controlled by the owner. A DAT acts as an immutable proof of ownership with an embedded digital signature. A digital trade with two digital inputs: the DAT of the seller and digital public money from the buyer; it results in a new DAT for the buyer. The trade is executed as a Delivery-versus-Payment (DvP) protocol using a digital"*fair exchange*" engine. In this protocol, the buyer uses digital public money to make a payment, with immediate finality, directly from buyer to seller, resulting in immediate settlement of the trade. The immediate settlement in the DvP results in a trade at internet speed, without involving a broker a custodian on any other intermediary, at effective zero marginal operational costs and without liquidity and other risks.

Keywords: digital asset, tokenised asset, digital public money, delivery-versus-payment, offline ownership.

JEL codes: O31, K23, G15.

1 Introduction

A rose is a *token* of love; a medal is a *token* of recognition; in the **Concise Oxford Dictionary**, a *token* is a piece of metal that can be used instead of a coin. A token, clearly, represents something of value to a person holding it.

The value represented by a token is owned by the person holding it: possession means ownership of the value the token represents. Digitally, with the token as binary data, ownership of a token, and hence of the value it represents, is recorded within the token data. This is needed because possession of data is never exclusive.

A digital asset token (DAT) is a data object that identifies both a specific, unique *asset* and its *owner*. It is an offline digital proof of ownership, held by the owner, stored in a computer operated by the owner. Almost like holding a physical token. An asset is anything of *value* that can be sold and bought. In a trade on an asset, the new owner obtains a new DAT and only the new DAT is valid.

DATs can be traded on a fully digital marketplace where digital money is used to pay for the trades. A Digital Public-Money Infrastructure (DPMI) provides digital "fiat" money for this market. This digital public money has offline ownership: the money is digital information stored in a dedicated, secure computer operated by the owner of the money, which recognises the owner to accept and then execute a payment instruction.[1] Possession of the device, en physically secured electronic device (e-vault) is a condition to use the money in payment. Annex A presents the DPMI with its objectvies and high level technical design.

The data in a DAT, the identification of a specific asset and of a specific owner, is cryptographically sealed—rendered immutable—by a digital signature. The digital signature in a DAT cryptographically proves ownership by the owner of the asset.[2]

The asset identification in a DAT is legally binding digital description of the benefits and duties accrued to its owner. This description identifies the (commercial) entity that created the token. It specifies the guarantees given by the token creator on the asset's persistent validity.[3]

For a purely digital asset, like a bond issued digitally, for instance by a bank or a government, the issuer is the DAT creator and that token effectively *is* the asset. For other types of asset, e.g. traditional securities, the DAT creator is the party that holds the asset in escrow.

Owners store their DATs on a personal hard disk or other persistent media. A DAT can be backed-up, or entered into an accounting systems, e.g. to be easily included in a balance sheet. A DAT is obtained by its owner by buying it from a selling party.[4] The owner is identified in the DAT by a public cryptographic key. The controlling, secret, part of the ownership key is stored in a secure way by the owner to give the owner exclusive control over the token and hence over the asset it represents.

[1] In the mid nineteen nineties electronic money with offline ownership has been issued in a number of countries by commercial parties, telecom operators, transit companies and also banks. The term electronic cash (e-cash) was used at that time for this digital, non-public money. Except for its use in transit, the e-cash deployments all failed commercially. This has been documented by Leo van Hove[12].

[2] This paper assumes a legal framework where a specially constructed data structure, like a DAT, has legal status.

[3] The legal and regulatory framework required to create a DAT with such guarantees for the identified asset is assumed to be present in jurisdictions where the assets will be held and the token created.

[4] The first selling party is the originator of the token.

The DPMI includes the provisioning of e-vaults to its users to provide them with effective offline ownership of their digital money. The DPMI public key infrastructure allows anyone to make and accept digital payments at any time, both face to face and over a distance at zero costs for the both payer and payee. A DPMI payment is realised as a publicly verifiable digital proof of payment. Digital public money can be denominated in any currency issued by a central bank.

1.1 This paper

This paper presents a novel delivery-versus-payment protocol to implement an ***offline*** *token arrangement*[5] where the sale of a digital token is implemented by the buyer providing a digital proof of payment to seller to trigger the automated uninterruptible completion of the transfer of ownership. This ownership transfer protocol does not require an intermediary. It relies instead on an easily scalable digital *"fair exchange"* implemented as a automated trusted process[2]. The fair exchange process realises the atomic swap of two digital data items: a payment versus a token, between the two parties. In support of this trusted processing a few bytes of status on each token is recorded centrally.

The first section presents a digest of some recent publications on tokenisation and assets. It highlights the difference with the approach to tokenisation in this paper.

Section 3 establishes the operational context for trading in DATs and the operational foundation for implementing DvP. Section 4 gives a detailed description of the steps seller and buyer perform, and the messages exchanged, to realise the atomic delivery versus payment of a token to a new owner for payment to the old one, leveraging the offline ownership of money provided by the a Digital Public-Money Infrastructure. This section contains an analysis of the safety and security of the presented DvP protocol.

Conclusion and suggestions for further work conclude the main part of this paper. Appendix A gives a summary of the key features of the payment system provided by the Digital Public-Money Infrastructure (DPMI) to bring digital public money to token buyers and sellers. This summary is complemented withe a high-level description of the system architecture and its key opperation: digital payment.

2 Other work

In 2024 the International Monetary Fund (IMF) published a working paper[4] by Victor Budau and Herve Tourpe with a conceptual model

[5]The term "token arrangement" is from [6, p. 4].

for a digital asset platform (DAP) to support a marketplace for assets represented by tokens with online recorded ownership.

The 2024 report[6] from the Bank for International Settlements (BIS)-Committee on Payments and Market Infrastructures (CPMI) to the G20 provides a model for tokenising real or financial assets. A token in this report is defined as an *entry in an online database* that *represents something of value*. The report specifies the database as a "ledger." A ledger is defined as the implementation as a programmable platform for recording transactions and ownership . In this specification programmability is needed in order to support, possibly required, additional token-type-specific operations during an online ownership transfer.

In December 2024 Ulrich Bindseil et al. note[3], in a critical review of terminology in the field of digital decentralised finance, that the term a *token*, as a record of ownership for some asset on a ledger, which is a shared, persistent, online repository of information, does not fit well with the Oxford Dictionary definition of a "*token*" as an object representing value that can be carried by its owner.

In the report[1] "*Tokenization and financial market inefficiencies*," published by the IMF, Itai Agur et al. present possible benefits of using digital tokens to represent assets, e.g. to reduce friction in trading them.

Cisar et al. [5] provide, in the introduction of their paper, an overview of the various proposals made in the past decades to reduce transaction cost of asset trading. They identify blockchain technologies, i.e. ledgers, as promising in this respect. Their paper adds to this body of literature on blockchain-based tokenisation of assets, with a focus on intricacies of tokenising the bond market on such a commonly accessible online infrastructure.

In 2025 Organisation for Economic Cooperation and Development (OECD) published a paper[11] analysing possible reasons for the absence still, despite of many proposals, of a market for tokenised assets, proposing policy considerations for financial supervisors and policy makers to facilitate its adoption.

Experts from central banks in South America, in a working group of the BIS-Consultative Group on Innovation and the Digital Economy (CGIDE) on expected benefits of tokenisation, present a report[10] on how Central Bank issued money should be the preferred way to pay trading asset tokens. The report presents the concept of a "Unified Ledger" which, they postulate, will become available in the near future. The "Unified Ledger" will be composed from multiple different ledgers. Aided by a hypothetical "unified inter-ledger protocol", this unified ledger can record tokens as transactions that involve both assets and fiat money. The costs of the extensive new infrastructure to realise the "Unified Ledger" would be covered by the high returns, expected by the authors, from operating a tokenised asset market with payments

in fiat money.

In contrast to the online, ledger-based approach in the literature, this paper defines ownership as *offline* for an asset as a DAT; complemented by digital public money for use in payments that is also owned offline. It presents a shared a dedicated automaton to deliver an atomic Delivery-versus-Payment. This automaton, realised as trusted process with a provably-correct implementation, obviates the need for a third party, i.e. a ledger, as source of truth on asset ownership: Ownership is included in the sealed, offline token data.

3 A digital token market

A marketplace for DATs has two stakeholders: owners and originators.

Owner: an entity that owns one or more DATs and may from time to time engage in buying or selling them;

Originator: an entity that creates DATs and makes them available to be bought.

In the IT system that implements the token market, stakeholders are pseudonymous users; they need only to be known by a public cryptographic key. That key will primarily be used to authorise an eventual sale; it may be used to claim benefits from ownership of the asset, e.g. coupon payments.

A DAT marketplace may have rules on who can join as owner. In some markets identity information may needs to be recorded to be admitted, e.g. as required by regulation applicable to an asset class. Identity data is not required to transfer, or accept, ownership of a token.[6] User information may need te be used when entering into the sales agreement that will be executed by the ownership tranfer.

An originator either holds real assets or virtual ones, e.g newly created, to be represented by a DAT. Originators are well known, e.g. by certification, by owners and potential owners; they typically give explicit warrantees on the quality of the asset backing each DAT. They also collectively create, or enable, the digital marketplace for their tokens. Originators are typically permissioned participants in the token trading system; consumer protection and other regulations may often be applicable to an entity aspiring to be an originator.

Owners can engage in trading with one another; in a trade the seller proofs ownership of the token with its private cryptographic key matching the ownership data contained in it. The price and other conditions

[6]The aggregating receipt token (ART) has been created with a pseudonym for the owner of the digital money it holds, in this case the seller; for an enforcement action, e.g. for Anti Money Laundering (AML), a regulator could unmask that pseudonym. A buyer could be identified in this way after the DAT has been sold.

for a trade may be established in any way that suits both parties at a suitable time before the ownership transaction. A DAT marketplace can, for instance, be realised on the basis of a social media platform extended with price forming and trade-agreement support functionality. An agreement for a sale is between the seller and the buyer, and a transfer of ownership happens with a direct payment in DPM. The digital payment of the amount agreed for the sale is an integral part of an atomic process for ownership transfer. The agreement can specify a time window for initiating the execution of it to allow a buyer to obtain the necessary liquidity.

3.1 Fair exchange

In computer science a digital token trade can be recognised as an instance of a "*fair exchange*" [2, 9] of digital data between two parties. In a fair exchange both parties either get both what they asked for or neither of them receives it. There is a formal proof by Garbinato and Rickebusch[7] that a digital fair exchange requires the involvement, in some form, of a third party to guarantee these two possible ways of completion the process. The cited paper describes this third party as an "*trusted process*".[7]

The *trusted process* in the transfer of ownership of a DAT against a payment in digital money is provided by an Token-Status Register (TSR). The TSR is an automaton implementing the state engine with two states shown in fig. 1. The TSR records the token and its state; if locked the TSR additionally stores the unlocking conditions

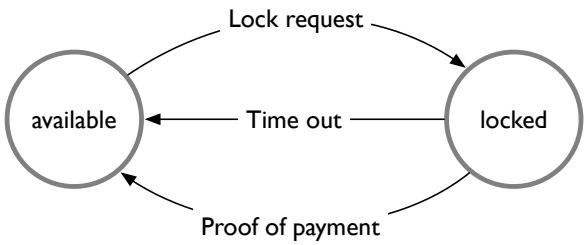

Figure 1—*State transitions for the token Token-Status Register.*

The automaton implementing the TSR responds to two specific digitally signed messages: One to finalise the trade with a payment; and another one to mark it as under agreement to be sold. The last messages locks out any other concurrent sale while awaiting the payment message; the first message implicitly marks a token as available for a future sale by the new owner.

[7] A trusted process can be implemented in a range of different ways, e.g. as database operated by a trusted third party or as distributed process operated by some, or all, stakeholders This. paper presents an automaton backed by a database as the implementation.

The Token-Status Register is accessible by all stakeholders. It also supports a query that returns a token for a specified asset/token identifier, if it exists, with its locked-or-not status.

The locking message to the TSR is signed with te ownership key, it additionally specifies the ownership key for the prospective owner; it results in a reply with a *proof of locking* message. The message finalising the token sale is a proof of payment for the agreed price, which als has been specified in the locking message. The proof of payment has been signed by a secret payment key in the the buyer'se-vault.[8] In processing these two messages, the TSR implements the trusted process in the *fair exchange* of DAT ownership.

The state engine implemented by the registry assures that the transfer of ownership is effectively atomic: A lock on a token in the registry is removed when either

- a payment has been received by the old owner[9] and a new token has been created proving ownership of the asset by the new owner, or
- the buyer has not made any payment and the old owner can offer the token for sale again.

The TSR guarantees finalising the transfer of ownership. It does so by validating the digital proof of payment, made in the expected digital currency, that matches the recorded price agreed between buyer and seller.

3.2 Data structures

Figure 2 shows key data elements in the design of the DAT ownership transfer protocol. Data elements that are necessary for the secure implementation of this protocol are shown in bold; data elements that represent data structures that are referenced by a hash are shown in italic.

As shown the figures includes some design choices, like the use of a **DAT id**. Showing some data elements as optional is to indicate the data as not required to formally prove the protocol correct. The figure is an illustration as actual data structures will be defined in a system implementation design based on a detailed operational and security requirements.

A DAT requires four data elements, a version number, an asset description, the public key of its owner and a digital signature over the data in the token. A reference to details of the contract for buying the

[8] See fig. A.2 in annex A for details on this digital payment.

[9] The proof of payment in the unlock message is recorded in the registry as a publicly accessible proof of the token price. If it has not been received directly from the buyer, the seller can retrieve the sale proceeds from the registry.

token, the price paid and the date it was bought can be included in the DAT.

As mentioned above, a Token-Status Register records status for each DAT. This requires three data elements: the asset for which the DAT is the proof of ownership; the version of the token; and the condition of being locked. The locked condition can conveniently be represented by a date and time in the future, for being locked, or a date in the past, for being available for trading. Using a date automatically unlocks the token at time out; if unlocked by a payment the date in the record is set as the current time. Initially this value is set to creation time of the token. For robustness and auditing purposes, the status record could contain the owner key, the payment received to unlock and details of the locking message for the transaction of which it records the result. The recorded payment guarantees that the seller can obtain the payment any time after the sale; this could be needed if communication breaks down.

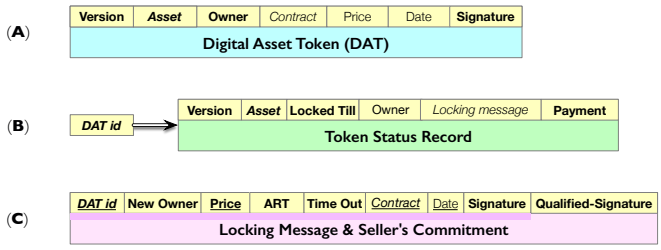

Figure 2—*Key data structures for the implementation of a fair exchange of asset ownership.*

A tokens status record is referenced by a **DAT id** computed as the hash of the asset description and the version. After creating a new token and its status record, the **DAT id** as index for the previous version can be removed.

The seller's commitment (c.f. section 4), is a message from the seller with a detailed agreement with the sale of an asset it owns with a legally binding digital signature. This qualified signature is over a locking message, which is marked with a band in a darker colour. The locking message is digitally signed by the seller using its ownership key for the token to be sold.[10] Data elements that have been underlined reflect the essential data points in the agreement, which need be verified by the buyer before making a payment.

3.3 IT infrastructure

The IT infrastructure for trading in DATs consists of the following components:

Marketplace an online meeting space where an owner can offer a token for sale and where potential owners can buy one;

[10] An owner can generate a fresh ownership key for each token.

Token-Status Register (TSR) a server with an automaton implementing the fair exchange of payment-versus-delivery of token ownership, which is backed by a database to record the existence of a token;

Ownership key a cryptographic key specifically used to associate a token to a specific owner for authorising an eventual sale;

DAT a cryptographically sealed data structure persistently stored in the memory of one or more computers owned by, or operated on behalf of, an owner;

Electronic purse (e-purse) the secure software abd hardware to store DPM and to make and receive payments for owners in a DAT trade;

The TSR is the trusted process that is involved in every trade. A token is recorded in the registry indexed by a unique identifier that can conveniently be generated as a cryptographic hash over the description of the asset represented by the token. The register is only concerned with the state of any possibly ongoing ownership transaction for each individual token. Except for a pseudonym, in the form of a stakeholder key, that can be different for each token owned, no identity information is recorded for an owner.

Stakeholder keys are specially generated to be recorded in transaction data as anonymous references to an owner to be used to exercise control in a future transaction. Stakeholder keys are implicitly certified by being recorded in the TSR.

In addition to the stakeholder key, an originator has a long-term cryptographic key that identifies it as a well known, trustable party with a key certificate generated in a suitable Public Key Infrastructure (PKI). This key is used to sign the legally binding description that defines the asset represented by a DAT. The TSR itself also has a certified, long-term cryptographic key used to sign the messages it sends.

4 Transfer of ownership

Figure 3 shows the steps in the protocol for a fair exchange of digital payment for ownership of a DAT. In the first phase of the protocol parties establish a sales agreement that meets the legal and regulatory requirements for a sale of the kind of asset the token represents.This agreement is the foundation for both parties to engage in the second, DvP, phase, which can start within an agreed time window.

The sales agreement can be based on a template that contains the asset description and any legally required stipulations, which can be provided online as one of the functions of a digital marketplace for assets. It also details the price to be paid by the buyer and the parameters

of the transfer process, like the digital identifier for the DAT and an identifier for the legal entity of the seller.

The online marketplace may record identies of its users to facilitate token trade where identity verification is needed. In this way, the marketplace software can then provide the seller with all required inforation to validate the buyer as a suitable prospective owner. To protect privacies identities could be in the form of pseudonymous credentials issued by a third party.

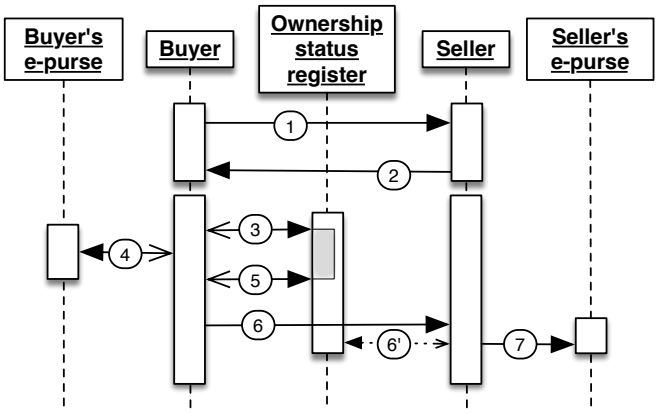

Figure 3—*DvP protocol for a DAT.*

The first two message in Figure 3 are digitally signed commitment that confirm the sale agreement. The marketplace software also can provide a service for parties to make the agreemnet legally binding, e.g a PKI for "qualified" digital signatures.[11]

The steps in the delivery-versus-payment protocol are:

1. **Commitment to buy** Buyer commits to pay a specific amount denominated in an agreed currency for a specific asset to be bought before a specific time;
2. **Commitment to sell** Seller confirms its obligation to sell the specified asset in a message to the buyer that includes a *locking instruction* for the TSR (See (**C**) in fig. 2);
3. **Lock asset** Buyer sends the locking instruction from the previous, which contains the token to be sold and payment data, to the TSR and obtains a proof of locking;
4. **Proof of payment** Buyer uses the e-vault in its e-purse to transfer the agreed sum to the seller's ART to create a proof of payment;
5. **Claim ownership** Buyer sends the proof of payment from the previous step to the TSR and obtains a new token in response;
6. **Finalise payment** Buyer sends the proof-of-payment to the seller;
7. **Redeem proceeds** Seller redeems the received proof of payment with the e-vault in its e-purse to add the funds to its spendable balance.

After step 2 the agreement is ready to be executed. The buyer initiates this in step 3 by sending the locking instruction received from the

[11]Details on how the contractual binding nature of an online agreement may be achieved will depend on jurisdiction(s). Such signatures serve to conform to auditing rules; they do not play a role in the share sale protocol.

seller in the step before to the TSR. The registry validates this instruction and then locks the ownership status. Figure 3 shows the locked status for the specified token in the registry as a small grey box.

A locking instruction for a specific token status is valid if i) the token is unlocked -AND- ii) the ownership key matches the key reference recorded in the token -AND- iii) the instruction has been signed with the seller's ownership key -AND- iv) the lock instruction has not yet expired. In locking the status, the registry records unlocking conditions. The locking instruction specifies the unlocking conditions as i) the payment details needed to validate payment by the agreed buyer and ii) the time-out time. The locking instruction expires when it is received after the time-out time; this time will be set by mutual agreement to allow the buyer enough time to overcome local technical issues in completing the transaction without undule keeping the seller waiting for its payment

The result of step 3 is a signed message confirming the locked status and the unlocking conditions. A digital signature with the registry key makes this reply a *proof of locking*. After validating the proof of locking, the buyer obtains a proof of payment to the seller of the agreed amount from its e-purse in step 4 by sending it the ART contained in the locking instruction.

With the completion of step 4 the payer has irrevocably made a payment to the seller. The next steps are to communicate this fact to both the TSR and the seller. Sending it to the TSR will release the token for its new owner; the seller uses it to add the money received to its spendable balance of digital public money, which can be done at any convenient later time.

In step 5 the TSR receives the proof of payment. After recognising that as the expected, valid payment, the registry computes a new token with the buyer as the new owner and sends it to the buyer in response. Upon sending the new token its ownership status is unlocked, ready for a future sale by the buyer.

With step 6 the buyer sends the paid amount to the seller. The seller, in step 7, then sends the received funds to its e-purse to make them available for further spending. If for some reason the message 6 has not been received, the seller can obtain the payment by asking the TSR for the token, which contains the proof of payment Figure 3 shows this recourse action as 6′.

Step 5, on one hand, and the two steps 6, 7, on the other hand, perform the asset side and the money side, respectively, of the delivery versus payment. Until step 4 the buyer can back out; the agreement in step 1 may have specified what parties should do in this case.

The duration of the ownership transfer is expected to be less than a few seconds. It is primarily determined by communicating the four messages in steps 3 and 5 to a server on the intenet. The computations

in precessing messages 3, 4 and 5 are expected each to be about a millisecond. For the seller the transaction process is longer than for the buyer by the time needed to transmit the message in step 6.

After completion of a transfer the TSR can publish a summary of the transaction to the web site(s) that implement the digital asset marketplace. That way these websites has actual information on the price and the liquidity in the market. This publication can also be done periodically, like ever hour.

4.1 Safety and security

Operational security, accessibility, availability and resilience of the TSR service can be provided by implementing it in a secured data centre operated by a neutral party, e.g. a share exchange or the central bank. Different types of assets may use different methods for implementing a type-specific TSR to match trade volumes and liquidity. For instance, to enhance resilience, based on traditional peer-to-peer, e.g. sharding, processing techniques the TSR could be deployed over a network of collaborating processing nodes. These nodes could be operated by stakeholders, e.g. asset originators, as a form of sharing cost of the trading infrastructure for their tokens.

The protocol is a version of a two-phase locking process[13]. The locking message is the first phase; it records all data required to complete the transaction. The lock prevents the selling of a stale token or double selling. The digital proof of payment is the final phase of this process; a new token is a proof of this. Recording the proof of payment in the TSR guarantees that the seller will always be able to receive payment. The two-phase locking also guarantees a *fair exchange* that is immune for interruptions by natural disasters and attacks.

With a resilient TSR, the protocol is fail-safe. It can be aborted by the buyer before step 4; it cannot prevented from completing after that step. Both steps 3 and 5 aree idempotent and can be repeated to overcome interrupted communication. Resilience in the TSR implementation must guarantee that the message initiating step 5 can always be received for any locked asset, e.g. by extending the time-out with the duration of an outage.

Security of the fair exchange of ownership of a token for a digital payment is further based on:

1. the security of the used cryptography;
2. the security of the authorisation for the payment in e-purse;
3. the security of the proof-of-payment for the payment in e-purse;
4. the correctness of the implementation of the TSR;
5. the correctness of the implementation of the marketplace software.

Cryptologic analysis and formal proofs of correctness provide a basis for trust in these aspect of the token market implementation.

Cryptography is used to compute digital signatures and hashes, using standrad algorithms implemented in standard libraries. The public keys used as ownership keys are certified by including their hash in the token.

Security of payment authorisation and its proof are essential properties for a DPMI.

A formal, i.e. one with mathematical rigor, of the protocol in its interaction with the TSR can be developed identifying the essential details for correctness of its implementation. In particular, this model will support a formal proof of correctness Delivery-versus-Payment (DvP) implementation. and hence of its security.

Resilience in operating the TSR can be enhanced with distributed deployment of the same correct implementation. The complementary synchronisation needed for distribute processing can also be proven correct.

5 Conclusion and future work

Digitalisation of assets can be realised by creating digital tokens, DATs, to represent them in data processing. With asset tokenisation a fully digital market can be realised where digital money is used in asset trading. Digital public money in the form of electronic cash (e-cash) enables the immediate, atomic settlement of tokenised asset trades; it integrates the digital asset market neatly in the wider economy.

A *trusted process* process is required to realise a token trade; this process is implemented by a Token-Status Register (TSR) that is accessible to all stakeholders. The TSR leverages aggregating receipt token (ART) technology in a DPMI to provide an instantaneous atomic delivery-for-payment of the asset. In a DPMI a DAT can be paid for in any currency issued in that form that the seller can accept.

Neither a smart contract, nor blockchain nor cryptocurrency is needed to implement the DAT marketplace and TSR. Ownership of both DPM and tokens is offline; the owner's e-vault act as custodial device for both its digital money and any digital tokens.

The fair exchange structure underpinning the asset trading protocol can also be applied to other types of transaction, for instance, a transaction to encumber the token with a loan, trading in bulk in a specific asset, like bonds issued by a bank, claiming a benefit from the asset originator like interest or dividend, or the sale of balance-type tokens, e.g. representing a number of shares in a company. This implementation structure could also be used to realise an atomic *payment-for-payment* in

an DPMI-based currency exchange. These applications are topics for further research.

Applying DPM as the digital payment in a trade of online tokenised assets, i.e. assets with ownership centrally recorded on a ledger (Distributed Ledger Technology (DLT)), could be realised by implementing the TSR in the smart contracts that manage the various types of assets on different ledgers. Identifying the type of asset where offline ownership would not be appropriate, e.g by the complexity of the process of creating tokens for them, and incorporating a TSR in the code that manages these assets, might be worthy subject for research.

The legal context for a DAT as a sufficient proof of ownership of an asset and of the status of a fully digital might be interesting for lega scholars to explore. The liabilities, if any, of the operator of the TSR while not being an intermediary might also be researched.

With offline ownership of the asset and immediate settlement with the TSR two of the four functions for a central securities depositories (CSD) have become obsolete. Research in how the other two CSD tasks, tracking assets and their issuers and owners, can be refocussed to keep protecting market participants in the context of fully digital assets with offline creation as tokens and immediate settlement in trades may be important.

Other research could focus on formally proving the correctness of the exchange structure with various refinements into its possible applications on different types of assets. Research could also address the business aspects and implementation options possible for implementing and operating the TSR .e.g. focussing on resilience and robustness.

Bibliography

[1] Itai Agur et al. *Tokenization and Financial Market Inefficiencies*. IMF Fintech Notes 2025/1. International Monetary Fund, Jan. 2025.

[2] N. Asokan, Matthias Schunter and Michael Waidner. 'Optimistic protocols for fair exchange'. In: *Proceedings of the 4th ACM Conference on Computer and Communications Security*. CCS '97. Zurich, Switzerland: Association for Computing Machinery, 1997, pp. 7–17. ISBN: 0897919122. DOI: 10.1145/266420.266426. URL: https://doi.org/10.1145/266420.266426.

[3] Ulrich Bindseil, Charles-Enguerrand Coste and George Pantelopos. 'Digital money and finance: a critical review of terminology'. In: *SSRN* (2025).

[4] Victor Budau and Herve Tourpe. *ASAP: A conceptual model for digital asset platforms*. Working Paper. IMF, Feb. 2024.

[5] David Cisar et al. 'Designing the future of bond markets: Reducing transaction coststhrough tokenization'. In: *Electronc markets* (Jan. 2025).

[6] experts in BIS and CPMI. *Tokenisation in the context of money and other assets: concepts and implicationsfor central banks*. Tech. rep. BIS–CPMI, Oct. 2024. URL: https://www.bis.org/cpmi/publ/d225.pdf.

[7] Benot Garbinato and Ian Rickebusch. 'Impossibility Results on Fair Exchange.' In: Jan. 2010, pp. 507–518.

[8] Eduard de Jong. 'How the King returns: a digital future for cash'. Version 2; Unpublished. Jan. 2024. URL: https://eduard.dejongfrz.nl/papers/latest-howkingreturns.pdf.

[9] Silvio Micali. 'Simple and fast optimistic protocols for fair electronic exchange'. In: *Proceedings of the Twenty-Second Annual Symposium on Principles of Distributed Computing*. PODC '03. Boston, Massachusetts: Association for Computing Machinery, 2003, pp. 12–19. ISBN: 1581137087. DOI: 10.1145/872035.872038. URL: https://doi.org/10.1145/872035.872038.

[10] Taskforce CGIDE. *Leveraging tokenisation for payments and financial transactions*. Tech. rep. BIS–CGIDE, Apr. 2025. URL: https://www.bis.org/publ/othp92.htm.

[11] *Tokenisation of assets and distributed ledger technologies in financial markets— Potential impediments to market development and policy implications*. Research rep. OECD, Jan. 2025.

[12] 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.

[13] Wikipedia contributors. *Two-phase locking — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Two-phase_locking&oldid=1263569407. [Online; accessed 20-January-2025]. 2024.

Appendix A Digital Public-Money Infrastructure

A Digital Public-Money Infrastructure (DPMI)[12] provides citizens, enterprises and government bodies a widely accessible digital system for payment with digital public money owned offline by its users. The central bank[13] issues the digital value that circulates in this system; this digital money is accessible to its users in a ways similar to solid cash: By receiving it in payment or by withdrawal from a bank account.

Managing the issuance and circulation of DPM closely resembles managing the solid cash system. Digital public money is also distributed with two tier model involving financial institutions. Except that with DPM there are no objects involved that need to be moved around securely in large volumes. Together with financial and other institutions the central bank is responsible for the continued trust in the system and its smooth, secure operation.

The DPMI provides:

Digital payments securely done in a direct digital communication between payee and payer, in any amount[14] by anyone to anyone at any time, over any distance, with immediate finality;

Offline ownership of the spendable money in an physically secured electronic device under control by the of the owner of the funds enabling payments directly from payer to payee without intermediation;

Privacy protection with anonymity of the payer and a strongly authenticated cryptographic pseudonym for each payee;

Security anchored in the hardware features of e-vaults storing money, cryptographic keys and vetted software that implements the value transfer protocol, complemented with active management of keys and system observation, detection and responses to potential incidents;

Inherent large capacity, strong resilience and robustness by the distributed nature of the secure devices, e-vaults, in the hands, or under exclusive control, of their users and a direct digital value transfer protocol between payer and payee with idempotent messages;

[12] This annex is a summary of my 2023 report, updated in 2024, "How the King returns—Building a Future for Cash"[8] that presents a comprehensive, detailed system architecture for a large scale digital money system with offline ownership.

[13] Or treasury as the case may be.

[14] The software in the device will be configured to respect a limit based on the assessed security of its hardware protection.

Enforcement of AML measures through pseudonymous analysis of the expired payee credentials, wich are regularly re-issued to users, that record received payments;

Digital payment integration in IT systems with a digitally signed proof of payment that transfers digital funds from a payer to a specific payee for a specific reason, which can be publicly verified, recorded in an administrative system and reverified for auditing.

A.1 System architecture

The IT system that provides the basis of the DPMI as a payment system consists of two distinct components: i) an e-purse to provide users with the functionality to make and receive payments; and ii) the issuer to provide liquidity, to manage the provisioning of e-vaults and enrolment of users and to manage system security, including the continuous re–provisioning of key certificates for payment keys to payees and of payee credentials to payees. There is a single issuer an many, many e-purses: one for each citizen, possibly one for each family and at least one for each enterprise and government agency.

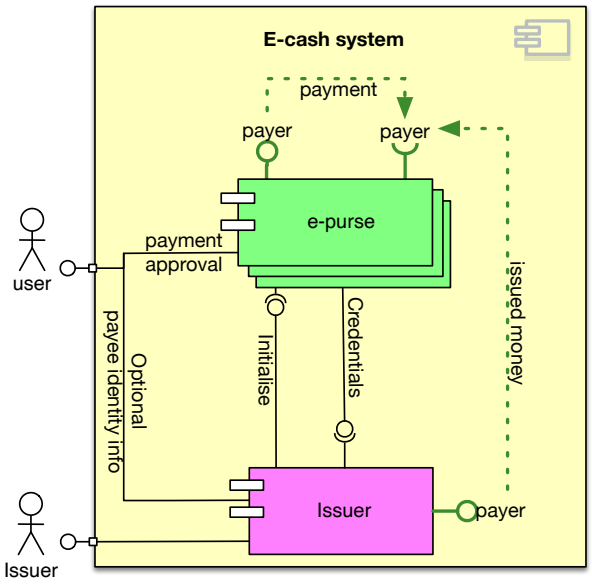

Figure A.1—*The two functional components in the implementation of a DPMI.*

The e-purse is the only component that handles money: it makes payments and receives them. An e-purse can be integrated into any IT system, enabling it to receive digital payments. Payments can be made by an IT system with an integrated e-purse by configuring the applicable payment authorisation structure in the e-purse. In this case, the e-vault can be configured to cryptographically authenticate user credentials.

An e-purse contains a secure hardware component to store a balance, secret cryptographic keys and specially vetted digital payment software. Computations critical for the security of the digital money, e.g. a digital signature in a payment, are delegated to the e-vault.

The issuer component, in its function as an actual issuer of digital money, operates a specially prepared e-vault that can make a payment

without a balance to the issuer's operational e-purse. The operational e-purse of the issuer is used to provide liquidity to financial institutions and other agencies that have an account at the central bank. The issuing e-vault is typically stored inside a vault and only used incidentally, typically with a security focussed *issuance ceremony*.

Many of the issuer operations are delegated to agents that in the course their business already interact with customers that are users of DPM. Banks, for instance, in addition to supporting their customers to make deposits and do withdrawals in DPM can provide them with the necessary payee credentials on behalve of the issuer.

Maintaining the database of Know Your Customer (KYC) data for users with the identifiers for their issued e-vaults could be doen by a special independent agency. Analising the received payment data for money laundering patterns can be done by agents.

Monitoring system operations for monetary data gathering or to detecting and respond to a potential security incidents could be done by the issuer in house.

A.2 Payment

Figure A.2 shows the two messages exchanged between payee and payer to make a payment. With the first message the payee informs the payer of its (pseudonymous) identity via one of its ARTs. The second message contains a proof of the payment, digitally signed by the payer's payment key certified by the central bank. The two e-purses in the figure contain for each user an e-vault to store spendable funds and secret keys. An e-purse contains the software to communicate with other e-purses and with the user; this software can run on any user device, e.g. a mobile device. In the payment, only the payer needs to access the e-vault, the payee can accept the payment in software by validating the public key signature on the proof of payment.

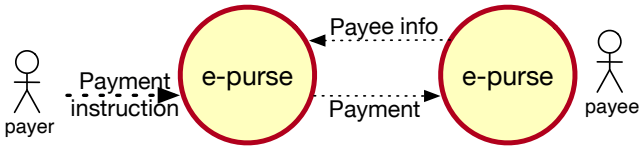

Figure A.2—*A complete e-cash payment in ART technology is final after just two messages.*

The two payment messages can be conveyed in different ways: as a QR code, via NFC, or added to a Universal Resource Locator (URL).[15] Each of the messages could be transported differently. The payment can be face-to-face or at a distance; the distance between parties affects how

[15] A URL is the address of a website. The URL format standard supports additional data for perusal by the webserver, i.c. as a payment.

the payment messages are transported between their respective digital equipment.

Distributing ARTs to users is part of the issuer's security management process. Payment key certificates and ARTs expire,[16] regularly issued and refreshed by the issuer as needed.

An DPM payment is atomic and idempotent;[17] its computation results in a digitally signed *proof of payment* that can be verified by anyone.

A.3 Payee info & aggregating receipt token

The payee info in fig. A.2 is a cryptographically sealed data structure called aggregating receipt token (ART). An ART is a security token that enables a payee to receive up to a specific number of payments from any payer, within a specific time and up to a *aggregate* total of payments. Each time it is used in a payment, it is extended with payment specific data, e.g. an invoice number, and its aggregate value is increased with the amount of the payment. A blind digital signature by the payer's payment key over the extended token data creates the proof of payment to be send to the payee as the payment. A received payment is added to the balance of spendable DPM by presenting its proof of payment to the owner's e-vault.

An ART is, typically, created by user-facing agents that operate "*Token Factory*" servers for that purpose. Upon creation an ART contains its aggregate value as zero, a validated payer pseudonym, the unique identifier of the payee's e-vault and specification of minimum and maximum payment amounts in can be used for. It also specifies the cryptographic algorithm to be used to create a suitably strong proof of payment.

A user obtains a bundle of ARTs that matches its usage profile upon enrolment; the ARTs is stored in the memory of the computer(s) that operate the e-purse software. The e-purse manages ARTs, selecting one appropriate for a next payment to be received, and detecting ones that are ART close to expiry.

When a ART is expired, the e-purse software constructs a refreshment command for a suitable token factory. A refreshment command is authenticated by the user's e-vault; it includes any expired ARTs.

[16] It is a system security management tool in the from of an expiring capability issued, and reissued, to a user upon in a request authenticated by the user's e-vault. An ART acts as a permit for a user to receive an amount of digital money over the period of its validity.. A user typically avails of a number of ARTs with overlapping validity; they are automatically renewed.

[17] An idempotent process is one that can be repeated as often as needed. The process has the same result each time. For a digital payment idempotency means that the same payment instruction can be issued repeatedly resulting in only a single money transaction. An idempotent payment is imune against data loss in communication.

The aggregating receipt token is the key technical feature that enables offline ownership of digital public money by providing an atomic, idempotent transfer of value form payer to payee.

A.4 The e-vault

After provisioning, the e-vault is owned and operated by the owner of the funds it stores; it is manufactured for the issuer and provided to users with a secure issuing terminal operated by an agent.[18]

An e-vault can be built with different levels of physical security to match different user intentions for the amounts to store and pay. For consumers a small, portable e-vault with tamper detecting hardware offers protection up to amounts of DPM that occasionally may be needed. All the various built forms of e-vaults have been programmed with the same ART-based payment protocol, shown in fig. A.2. The software will be configured with maximum amounts reflecting the security class of the device.

An individual owner controls spending of DPM funds witha e-purse software installed on a personal device. Control of corporate DPM funds in its e-vault, e.g. can be integrated in the administrative system and configured in accordance with executive financial responsibilities. Financial institutions, for instance, own DPM to support withdrawal and deposit by their customers. In the same fashion, central bank supports lumpsum DPM payments into or from their reserves.

A.5 Summary

- ☞ The cryptographic **proof of payment** to a specific payee as the result of an atomic payment computation in the e-vault;
- ☞ A **public-key validation** of this proof of payment, which allows any third party to ascertain that a payment of a specific amount has been made to a specific entity;
- ☞ **Anonymity** of the **payer** in the **offline payment** process with local owner authorisation inside an e-vault.

[18] Issuance of an e-vault can be done similar to banknotes, i.e. via intermediaries. Banknotes can also be seen as "secure devices."