Abstract

In this paper we illustrate the relationship between ledgers and tokens in a complete CBDC solution that delivers fast, immediate, low-overhead payment, both on-line and off-line. We also present a technical basis for a manageable, scalable implementation that provides privacy by design and by default.

Ledgers and Tokens for Central Bank Digital Currency

Eduard de Jong & Peter A Cattaneo

version 1.0 (21.6.2023)

Keywords: electronic cash, e-cash, digital payment, offline payment, money, digital money, ledger, **CBDC**

Central Bank Digital Currency (CBDC) fills a gap in the technology available for Central Bank money.[i]

	Central Bank Money		Commercial Bank Money
	Cash	**Bank Reserves**	
Physical	Notes and Coins	Paper Ledgers Legacy/Obsolete	Paper Ledgers Legacy/Obsolete
Digital	CBDC	Digital Ledgers	Digital Ledgers

As on-line commerce has become a significant part of the economy, the void left by the lack of Central Bank digital cash has been filled by commercial products that place a number of burdens on society: high fees, loss of privacy, inappropriate targeting of consumers, theft, and exclusion of social groups.[ii]

Cash-like payment with a user experience that is seamless for both face-to-face (offline) and remote (online) payments is *the* essential function of Central Bank issued digital currency. Truly offline payment requires the use of a digital bearer instrument.

The system that issues and manages these payment instruments can and should support enhanced features. These additional features rely on the existence of the CBDC. To succeed, the initial focus must be on: 1) Payment; and 2) Adoption.

We propose a specific technical architecture that delivers all of these requirements: a managed *aggregating token*.[iii] This document provides an introduction to this architecture.

We also introduce the concept of using meta-data in this architecture to implement policies for specific groups of users and specified categories of transactions. This approach enables fine-grained tuning of the resulting system to meet the needs of the entire community. It also provides a mechanism for adjustment to optimize features that implement policies and to meet future needs as they develop.

Ledgers and Tokens

Modern payment systems rely on digital ledgers for account balances and high value payment transactions. This excellent architecture does not deliver offline payment. Ledger payments depend on 3rd parties and can only finalize transactions after connecting to the back end. *Aggregating token* technology is the evolution of the token-based solutions that have been developed since 1991 using modern cryptography to deliver the required payment experience along with all of the features required for a CBDC.

Boundaries and categories for e-cash use

A CBDC system must deliver a consistent user experience for payments. At the same time, the services if offers can, and will, have constraints that are specific to classes of users and the types of payment. For example, protecting privacy for a user paying 25 € or 250 € is essential. For a payment of 2.5M € privacy is not expected or required. The principle of diversity in use requirements has been noted by BIS and others[iv].

The aggregating token e-cash system we propose as CBDC has operational parameters that set and adjust boundaries for use. The definition of these boundaries and their management is an integral part of operating the system. Categories of users, limits for amounts, rate of transactions, and such are set at the initial deployment. The parameters can be updated later based on monitoring the operation.

To illustrate the concept, figure 1 shows a simplified diagram with payment-use boundaries in two dimensions, the amount and the type of user. The light colored area marked *Full Ledger* shows that high value transactions will all be between accounts on a digital ledger. In this area, businesses and consumers have no expectation of immediacy and unconditional privacy. Oversight for taxation and Anti Money Laundering (AML) is required.

As an example, figure 1 shows two areas for the use of e-cash:

1) *Managed* e-cash used by individuals identifiable by linking to their bank account;

2) *Free Use* e-cash that does not require an account or validation of user identity.

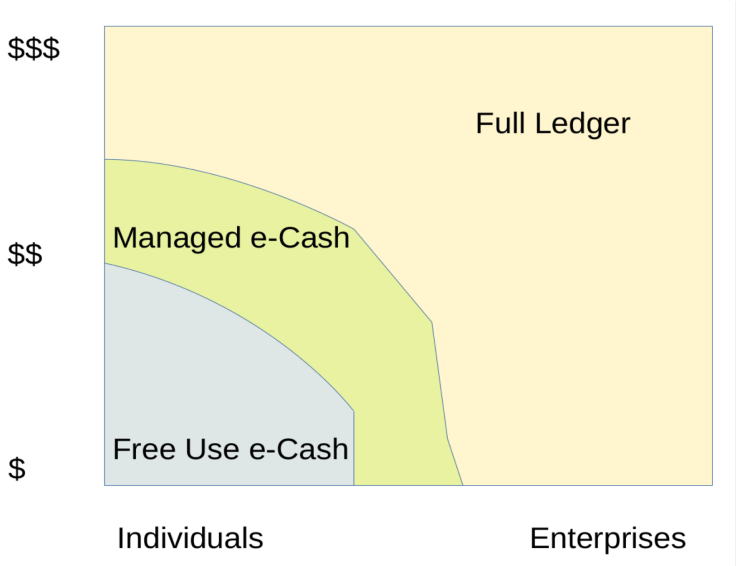


Figure 1: Boundaries for the use of e-cash

Managed e-cash delivers the benefits of e-cash, including fee-free, offline payment combined with automated online deposit or withdrawal from a bank account, as well as online payments to ordinary citizens and businesses who may, or may not, use the existing banking system.

Free Use e-cash delivers the same user experience for paying and receiving money online and offline to individuals and small businesses. With *Free Use* e-cash unbanked or underbanked users can fully participate in the digital economy.

A practical design for a CBDC e-cash system will support configuration of multiple dimensions with boundaries that may define additional categories of users and usages of e-cash including a distinction between different types of payers or payees, e.g respectively, an employer paying wages or a landlord receiving rent. Some of the configuration dimensions will be social, such as a requirement for KYC for payees making higher value payments. A unique configuration parameter provided by aggregating token technology is the ability to set limits on the velocity of money for different classes of payments. This technology can deliver enhanced features to e-cash such as complementary currencies, interest payments, multiple currencies, dispute resolution, and others.

In the design of CBDC there are challenging requirements and many choices to be made. This complexity can be addressed by realizing a faceted system that delivers an optimal experience for each category of users and the financial services they need.

Money Flow and Oversight Data

Two closely related areas of concern in a payment system are securing the actual flow of money and obtaining and responding to oversight data. In a ledger-based system, oversight data is available for every transaction. With e-cash payments, the flow of money can be different from the offline flow of oversight data. That these flows can be best implemented separately is one of the key insights that led to the development of aggregating token technology.

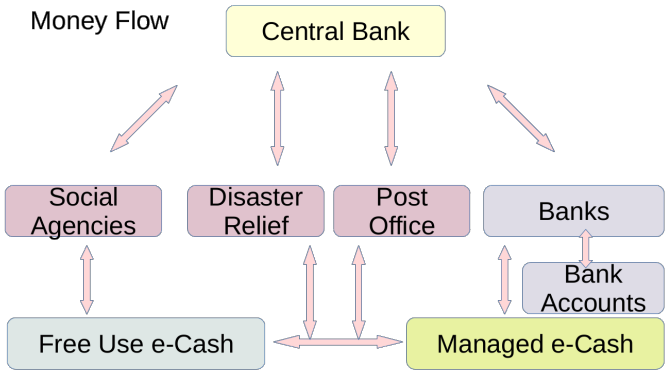


Figure 2; The flow of e-cash between users, agents and the issuing central bank.

Figure 2 shows the flow of money between users with an example of a number of special users that act as agents to pass on e-cash from the issuer to the users. The user experience is the same for all e-cash users, including the intermediating agencies. Deposits and withdrawals to bank accounts keep issued e-cash in circulation.

The agents and the central bank see the money that is issued and redeemed. E-cash payments between end users are not visible.

To manage the operation of the system, the *aggregating token* e-cash system provides the central bank with a secure data flow (figure 3). This data is designed for system oversight. To manage the system the Central Bank does not need to engage with intermediaries or to examine accounts.

Managed e-cash data will be anonymized. The mapping to accounts may be preserved for unmasking in appropriate legal circumstances.

Free Use e-cash is anonymous. In the event of inappropriate use, specific e-purses can be managed. But individual users cannot be targeted.

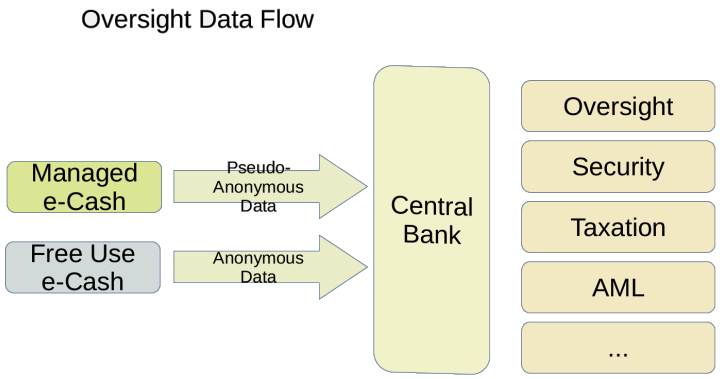


Figure 3: Flow of operational data for oversight with aggregating token e-cash

This data flow gives the central bank complete oversight into the operation of the system. Any failure, inconsistency, breach, attack, or other compromise of the system can be detected. This allows proper monitoring and response to any bad behavior. The *aggregating token* technology provides limits on the scope of any compromise.

Relation to Current Proposals

Every CBDC proposal includes a requirement for cash-like payment that is immediate, final, offline & online, and deliverable with no per-transaction fee. We believe this is essential for the success of any CBDC system and cannot be compromised in any dimension. A number of analysis have recognized the inadequacies of account-based solutions, DLT, and other technologies in meeting the payment requirements.[v] We propose a solution that does meets all of these requirements for payment.

Every CBDC proposal includes privacy as a fundamental principle. We believe privacy must be guaranteed by default and by design. We propose a solution that does not capture payer identity, so it can never be revealed.

System manageability is an essential feature of a CBDC system. We propose a solution that includes a complete, secure, dedicated data stream for the oversight and management of the system. It is cryptographically complete for security and management, but not does not include identity and other information that could be misused.

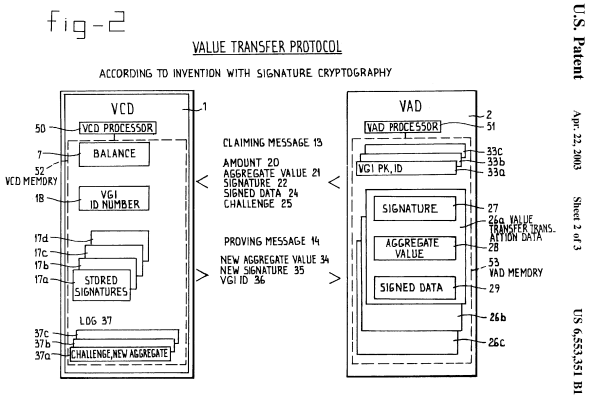
Many features are proposed for CBDC systems that go beyond cash-like payment with privacy. We view these as additions to the system that will change from time-to-time based on changing policy requirements. We believe that the core system must operate independent of these additional features. The system must support the dynamic addition and updating of these features.

Aggregating Token Technology

In the mid 1990s Chris Stanford and Eduard de Jong invented and patented[vi] technology for payment (*value transfer*) that is directly between the two parties. No external resources are required and it is finalized immediately. In addition to issuing digital value to the payers, the system issues *aggregating tokens* to the recipients of payments.

The novel value transfer (payment) protocol starts with the payee adding a cryptographic challenge to the amount requested. This reversal of the usual communication sequence provides major benefits:

1. The payer can securely see and verify the amount and the identity of the payee before authorizing payment.
2. The identity of payer can be excluded from the transaction.
3. The payee only needs software to accept payment.
4. The transaction is performed with just two messages: 1) the challenge request from the payee, 2) the confirmation of the payment from the payer.



5. The tokens issued to the payee can be created by a supporting agent.
6. A complete cryptographically secured transaction record for system monitoring and analysis is produced.

In addition to controlling the amount of e-cash in circulation, the central bank manages the properties of *aggregating tokens* that are issued to payees for the operation of the system. The policy choices for different categories of users are implemented in the settings of these tokens. The system functions fully offline until token limits are reached. When a token reaches time or transaction limits it must be exchanged, posting the transaction history in return for a fresh set of tokens. This is similar to the process used when physical bank notes are retired after use. This aggregating token exchange complements e-cash currency issuance, providing fine-grained oversight and control of the transactions.

As a true offline system, there is no cost for a payment transaction. E-cash circulates directly between users without intermediaries. No servers are required for high-availability, high-capacity, low-latency transaction processing. Issuance of e-cash currency and the *aggregating tokens* is only required periodically with modest system performance requirements.

Breakthrough Technology

Aggregating token technology addresses inherent limitations in other forms of digital payment. It delivers a digital bearer instrument that finalizes payments off-line. The system can be monitored and managed because it is *intermittently on-line*[vii].

By reversing the flow of information into a *pull* transaction from an *aggregating token,* the value held can only be spent once, and can only be redeemed by the owner of of the *aggregating token* used in the payment. If anyone intercepts the cryptographic data representing the payment, it has no value. Only the requesting token holds the keys to access the received value. This means that payments can be received using low-cost software-only solutions without expensive security measures. Any mobile phone or point-of-sale terminal can run the app.

Each payment is an idempotent operation. It can be transmitted repeatedly and applied multiple times, while guaranteeing that that value will be credited exactly once. This allows the use of one-way payment mechanisms such as QR codes. Payers can send payment through multiple channels to insure receipt. And they can confidently reply to requests for retransmission. All transactions are fully authenticated cryptographically.

Commercial History

Since their introduction in the early 1990s, e-cash systems have only been commercially successful in walled gardens. In these cases, such as transit payment, the issuer and payee for all users is one entity. This allows the use of simplified technology. While demonstrating capabilities in areas such as high volume transactions and security, existing products do not provide a basis for CBDC.

Various attempts have been made to offer open payment e-cash solutions. They have all failed[viii]. Because the issuer was not a central bank, key properties of the system were wrong: the issued currency was not widely accepted, transactions were monetized, private information was exploited.

The proposed *aggregating token* technology has been licensed, developed, and deployed commercially. Its acceptance has been limited because the primary benefits of the technology, including payer privacy, are not valued in the commercial market. For CBDC, the situation is reversed so *aggregating token* technology provides essential features.

System Operation

Aggregating token technology enables central bank control of e-cash as an IT system. The central bank is the issuer and the guarantor of the monetary value of the *digital information* exchanged in a payment. E-cash issuance and redemption are two of the primary operations of the system. A unique feature of a*ggregating token* technology is the direct control of both operations.

The issuer can delegate some of its operational functions to agents to agents that are already otherwise engaged with users, e.g. banks or social services.

Security for a large scale CBDC requires strong defenses, system operations monitoring, and effective incident response. Cryptographic algorithms, hardware security and management of cryptographic keys provide the basis for a strong defense. *Aggregating token* technology provides complete visibility of payment transactions through a cryptographically secured log for monitoring. Response to issues ranging from security to policy compliance is managed through control of the issuance of tokens and configuration of cryptographic keys.

The transaction log of *aggregating token* payments also provides an efficient mechanism for monetary controls.

Cost structure

Aggregating token payments are directly from payer to payee so there are no per-transaction infrastructure costs. This is essential to deliver CBDC that has no fees for payment transactions.

The payment infrastructure for *aggregating token e-cash* does not require any real-time, low-latency servers neither for authentication nor to implement ledgers. None. All infrastructure operations have modest bandwidth requirements, and are not affected by latency. This allows scaling to very large numbers of users at a reasonable cost.

The idempotent payment functions allow secure software-only receipt of payment. This dramatically simplifies and lowers the cost for merchants and others receiving payment. Any existing device can be used with a simple software upgrade.

A value in CBDC is exchangeable for the other types of money. Operating the infrastructure for this exchange has costs. With software-only upgrades this interface for e-cash minimizes operational costs. Withdrawal and deposits to a bank account for the user of e-cash are effectively e-cash payments from and to the bank, respectively. While ordinary payments have no fees, a bank could choose to charge a service fee for processing these e-cash payments as corresponding ledger entries.

Infrastructure and issuing costs for the issuer can be covered by seigniorage. Fees can be charged by agents that provide enhanced products or services.

In comparison to both traditional cash and bank intermediated payments e-cash as highly distributed IT system will have significantly lower overall costs.

Additional Features

CBDC discussions have included a wide variety of additional features to address specific policy goals. These include complementary currencies, insurance against loss, interest payments, multiple currencies, and dispute resolution. All of these features are supported by *aggregating token* technology. They can be introduced at any time during the operation of the system and updated as required.

One example is complementary currencies. An *aggregating token* system can implement multiple complementary currencies, support alternate or complementary payment in them and provide straightforward management.

Another capability is illustrated by multiple currency support. *Aggregating tokens* can support multiple currencies (each issued and redeemed by a central bank), with payment and receipt of payment in each currency. Alternatively, the technology can support automation of currency exchange.

Deploying a CBDC system is a major, long term investment. Over the lifetime of the system, the requirements will change. Aggregating token configuration enables adapting to these changes.

Conclusion

Governments and Central Banks around the world are examining the options for CBDC.[ix] All of these studies recognize that a primary function of a CBDC is payment that works both of-line and off-line. This requires using both ledger and token-based technology working together in a dynamic system that manages the boundaries of each to meet operational and policy goals. The resulting solution is e-cash that is better than physical cash.

> For users: Payment can be local or on-line. E-cash can be loaded remotely. E-cash can't be stolen and payments are only redeemable by the designated payee.
>
> For the Central Bank: Complete system oversight: transaction integrity, velocity of money, AML, security incident response. Wide range of intermediaries for different purposes. System enforcement of policy.

Aggregating token technology delivers this payment experience with a true bearer instrument for immediate settlement that does not require a real-time back end while providing system control. *Aggregating token* technology also provides a platform for dynamic value added services that complement the basic CBDC functionality. Features such as value back-up/insurance, dispute resolution, interest/demurrage, complementary currencies, and multiple currency support, are widely discussed as part of CBDC planning. Since these services are based on policy goals that will change from region to region and over time, they must be flexible and changeable without impacting the core functions of the system.

i CBDC is Central Bank Money
US Federal Reserve: https://www.federalreserve.gov/publications/money-and-payments-discussion-paper.htm;
European Central Bank: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

ii Many studies have identified negative factors in existing digital payment options. All government and bank studies identify one or more of the issues listed, particularly fees and privacy. Studies that focus in this area include:
Veblen Institute *A digital euro for a better monetary system* https://www.veblen-institute.org/IMG/pdf/veblen_study_digital_euro_the_case_for_a_public_option_jan_2023.pdf
MIT, Maiden Labs: *Expanding Financial Inclusion or Deepening the Divide?* https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/63c01f1bcf425f01973b4889/1673535260873/MIT+DCI+%26+Maiden+Labs+-+CBDC+%26+Financial+Inclusion+%28Jan.+2023%29.pdf
Federal Reserve Bank of New York – Monetizing Privacy
https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr958.pdf

iii Eduard de Jong, *Cash: The once and future king,* https://eduard.dejongfrz.nl/papers/latest-kingwillreturn.pdf

iv BIS: "...a CBDC could be fully anonymous for small value payments but not for large payments"; pg4
https://www.bis.org/publ/othp42_fin_stab.pdf

v Nearly all of the references incorporated here have some reference to limitations of existing payment technologies. Specific issues are covered by the Veblen, MIT, Maiden Labs, and FRBNY documents referenced above in (ii).

vi *System and method of cryptographically protecting communications* "A value transfer system..." EP0904581B1, https://worldwide.espacenet.com/patent/search/family/019865988/publication/EP0904581B1?q=EP0904581B1; US6553351B1, https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/6553351

vii a) BIS divides payments into three categories. 1) fully-online, which fail to meet CBDC payment requirements for off-line line use; 2) fully-offline, which fail to meet CBDC requirements for monitoring and control; and 3) intermittently-online or staged-online, which can finalized payments off-line and provide visibility and manageability. The BIS description of intermittently-online solutions is helpful in understanding the concept, but is based on an inferior design.
https://www.bis.org/publ/othp64.pdf
b) ECB concluded that "risks can only be effectively mitigated by means of regular online reconciliation of data"
https://www.ecb.europa.eu/pub/pdf/other/ecb.prototype_summary20230526~71d0b26d55.en.pdf

viii Failed e-cash systems include: DigiCash, Proton, Chipper, ChipKnip, Danmønt, Avant, Geldkarte, Moneo, multiple versions of Visa Cash, and Mondex
Many of these are discussed in the BIS Project Polaris report: https://www.bis.org/publ/othp64.pdf

ix Governments and banks with recent CBDC studies include:
European Central Bank
2020 https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf
2023 https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews230113.en.html
European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England Board of Governors Federal Reserve System, Bank for International Settlements
2020 https://www.bis.org/publ/othp33.pdf
2021 https://www.bis.org/publ/othp42.htm
Bank for International Settlements
– BIS Innovation Hub 2023 https://www.bis.org/publ/othp64.pdf
US Federal Reserve 2022 https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf
US Treasury 2022 https://home.treasury.gov/news/press-releases/jy0956
US Congress 2022 https://www.congress.gov/bill/117th-congress/house-bill/7231
US Executive Branch 2022 https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/
Bank of Japan 2020 https://www.boj.or.jp/en/about/release_2020/data/rel201009e1.pdf
Bank of Canada 2023 https://www.bankofcanada.ca/2023/02/staff-analytical-note-2023-2/
International Monetary Fund 2023 https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/04/12/IMF-Approach-to-Central-Bank-Digital-Currency-Capacity-Development-532177
Bank of England 2020 https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593&la=en
Reserve Bank of India 2022 https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1218
Bank of Ghana 2022 https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf