

Sovereign Grassroots Currencies: A CBDC Architecture for Credit and Monetary Policy (Full Version)

Ehud Shapiro

London School of Economics, UK, and Weizmann Institute of Science, Israel

Abstract. A Central Bank Digital Currency (CBDC) is central-bank money in digital form, held by the public. Leading designs have two limitations: conversion from bank deposits into CBDC can accelerate deposit flight, requiring safeguards; the CBDC stays outside credit creation and monetary-policy operations.

Here we present a CBDC architecture that overcomes these limitations, based on grassroots currencies. It has three components: (1) **Money:** *sovereign grassroots coins*, which are digital debts of one unit of fiat currency issued by the central bank, constituting a direct CBDC; (2) **Credit and Liquidity:** *non-sovereign grassroots coins*, which are digital debts of one unit of the same fiat currency, redeemable at par, that can be issued by any person, natural or legal — adding credit; and (3) **Interest:** grassroots bonds, sovereign and non-sovereign — adding maturity, and with it interest, standard banking instruments, and the central bank’s instruments of monetary policy.

The central bank can therefore lend, absorb liquidity, set its rates and buy and sell securities in the coins and bonds the public holds, choosing the counterparties and terms of its credit operations, and without converting bank deposits into newly issued central bank money on demand.

We prove that one unit of the fiat currency is the only arbitrage-free price of a grassroots coin whose issuer meets presentations, and argue that the central bank’s lending rate and the rate on its own bonds bound what its counterparties pay and accept on comparable terms; the central bank can choose to deal with any counterparty, not just banks.

Keywords: Sovereign grassroots currencies · Central bank digital currency · Mutual credit · Grassroots platforms · Liquidity · Monetary policy · Stablecoins

1 Introduction

A Central Bank Digital Currency (CBDC) is central-bank money in digital form, held by the public [11,14]. Leading designs have two limitations: conversion from bank deposits into CBDC can accelerate deposit flight, requiring safeguards [15,18,45]; the CBDC stays outside credit creation and monetary-policy operations [72].

The contenders. Of those in operation or in pilot we consider four, the Sand Dollar of the Bahamas [33], the eNaira of Nigeria [32], JAM-DEX of Jamaica [19] and the e-CNY of China [88]; the digital euro [45,46] is in preparation, with a pilot possible from mid-2027 and a first issuance during 2029, and the digital pound [17,18] is in design, with no decision taken on introducing it; and the research community has designed systems for them [78]: Project Hamilton [69], Chaumian eCash [25,34], and the privacy-preserving Platypus [90] and PEReDi [63]. Beside them stand the private alternatives, regulated stablecoins [1,2,56] and tokenised deposits [50].

The designs are classified by who holds the retail claim and who keeps the retail record [8,10]: in a direct CBDC the central bank keeps every retail balance and executes every payment; in a hybrid or intermediated CBDC intermediaries do, the central bank keeping a copy or a wholesale ledger; in an indirect CBDC the claim is on an intermediary, backed by central bank money. Each, and each private alternative, places one record and one party inside every retail payment.

Seven central banks and the BIS have set what a retail CBDC must satisfy [14]: three foundational principles—do no harm to monetary and financial stability, coexistence with cash and other forms of money, and innovation and efficiency—and fourteen core features, among them convertibility at par, availability offline, low or no cost to end users, instant settlement, resilience, scalability, interoperability, a robust legal framework and conformity with regulatory standards.

The two limitations. The first limitation is the subject of the central banks' own report on financial stability [15]. Deposits are converted into central bank money at will, disintermediating the banks, and a run into it costs less than a run into cash, so a systemic run may be faster and larger. How much so depends on the design of the CBDC and on the credibility of deposit insurance. The safeguards proposed are limits on holdings and on transactions, tiered remuneration and waterfalls into bank accounts.

The second limitation holds of all of them: credit creation and monetary-policy operations remain outside the CBDC, in bank money and reserves. That is a choice those designs made, not something a CBDC must be: interest-bearing central bank digital currencies have been proposed, and interest is an instrument of policy [5,26,40] (Section 6).

Grassroots currencies. Grassroots currencies [79], issued by natural or legal persons, are IOUs with the obligation to redeem issued grassroots coins at par against any grassroots coins held by the issuer. Liquidity forms by mutual credit: persons who trust each other swapping their coins, with no system-wide ledger or operator.

The proposal. Here we present a CBDC architecture that overcomes these limitations, based on grassroots currencies [79]. It has three components:

1. **Money:** *sovereign grassroots coins*, which are digital debts of one unit of fiat currency issued by the central bank, constituting a direct CBDC;

2. **Credit and Liquidity:** *non-sovereign grassroots coins*, which are digital debts of one unit of the same fiat currency, redeemable at par, that can be issued by any person, natural or legal — adding credit;
3. **Interest:** grassroots bonds [81], sovereign and non-sovereign — adding maturity, and with it interest, standard banking instruments, and the central bank’s instruments of monetary policy.

The three components are realised in one grassroots social contract [53]. Given a denomination, call it *Dollar* for simplicity, every person issues their own Dollar-denominated currency under it, and a sovereign grassroots coin is simply a Dollar-denominated grassroots coin issued by the central bank of the Dollar. There is no separate protocol for the central bank, and the only difference between it and other person-issued Dollar-denominated grassroots coins is that they all carry some risk of default, whereas a central bank can issue by fiat as many Dollars as needed to redeem their sovereign grassroots Dollars.

A *grassroots currency* comprises the grassroots coins and the grassroots bonds of its issuer; its coins are money and its bonds are credit.

Money. The central bank digital currency proposed here is the sovereign grassroots coins, a direct CBDC [8]: they enter circulation by exchange for fiat coins and by the central bank’s own payments, and leave it by redemption into fiat coins, the central bank countersigns every payment and records it in its own log, and the public holds a claim on the central bank and on no intermediary.

They differ in the machinery only from the designs in which the central bank keeps the ledger and settles every payment [18,45,69]: each person keeps their own holdings, the central bank keeps its log, a payment is disseminated over the social graph [67], and it is final when the central bank has countersigned it, with no consensus.

A payment is countersigned by the issuer of the coins paid and recorded in the issuer’s log, held by machines the issuer designates: for a person, state custodians chosen among their friends [44]; for an institution, its own.

A payment needs its payer, its payee, the issuer and those machines. So it proceeds over any network that reaches them, Bluetooth or a local network with no connection to the Internet; it is confidential to the three parties, and the custodians’ persons have no access to the log their machines hold; and it bears no fee required by the architecture, an issuer being free to charge for their services. The central bank sees only the payments in its own coins.

A person who loses their key or device recovers their identity from their identity custodians and their log, exactly, from their state custodians, and resumes without double spending [44].

A coin is a signed debt instrument, analogous to a promissory note, which is legally binding also in electronic form, with ordinary rules of contract governing the debt it states. Whether it is negotiable, and whether the central bank may issue it [17], are questions for each jurisdiction.

The coins create no credit and open no lending channel for the central bank, and they add no instrument of policy: remuneration and limits on holdings can be added, as in the other designs, and are not part of it.

Credit and liquidity. With the denominated grassroots currencies of persons, sovereign grassroots coins are the base money of the denomination [72]. Counterparties that issue coins of their own allow the central bank to issue its coins against them. In this component the central bank issues its coins by mutual credit lines.

Issuance that is not by conversion is Kumhof and Noone’s principle [65]: no guaranteed on-demand convertibility of bank deposits into the CBDC, and issuance only against eligible securities, principally government securities. There the central bank buys securities its counterparty already holds; here it lends against coins its counterparty issues.

A mutual credit line is a swap of its coins for the coins of the counterparty it chooses—a bank, a city, a firm, a cooperative or a household, any counterparty the architecture admits and its mandate allows—in the amount and at the time it chooses, with no bank between them and no account at the central bank.

The counterparty’s coins are redeemable against their holdings, and their coins in circulation are redeemable in full exactly when their holdings cover them [79].

As the central bank’s lending creates reserves today, its mutual credit lines create sovereign grassroots coins, and unlike reserves the public holds and pays them. The sovereign grassroots coins and bonds in circulation are at most what the central bank has minted and parted with, redemption into fiat coins reducing them and no demand of a depositor increasing them; maturity turns one of its bonds into one of its coins and adds no debt. They enter circulation only by transactions of the central bank, and thereafter circulate by payment, swap and redemption.

A swap of coins is at par, on demand and bears no interest, so the central bank has the counterparty, the quantity and the timing of the liquidity it provides, and no rate. Every other person creates credit independently of it.

Person-issued denominated grassroots coins are redeemable at par into sovereign grassroots coins along a chain of liquidity from their issuer to the central bank, and then by it into fiat coins. The only arbitrage-free market price of a coin that meets redemptions is one unit of the fiat currency, so, while redemptions are met, the currencies of the persons and of the sovereign are one currency, with the fiat currency as its unit of account.

Credit is created by every person, as inside money [30,72] secured by social collateral [20], which none of the designs compared allows; a bank issues its coins in place of deposits.

The central bank holds no retail accounts and takes part in no payment but in its own grassroots currency. Households, firms and banks accept payments in their own currencies, in the currency of the bank they are customers of, or in the sovereign grassroots currency. Banks settle among themselves by set-off and chain redemption, and need not settle every payment between them in central bank money.

Sovereign grassroots currencies add no on-demand operation that turns a bank deposit into newly issued central bank money: no holder of a bank deposit

has a right to newly issued sovereign grassroots coins, and a bank's reserves are the bank's own. A depositor obtains sovereign grassroots coins from a holder, which reallocates coins already in circulation, or from the central bank against cash their bank pays them, where the central bank elects to make that exchange, which changes the form of central bank money and not its quantity (Lemma 2.3). No limit, tier or waterfall is therefore needed to bound the demand-driven creation of central bank money, which the central bank issues at its own election; whether a limit is wanted for other reasons — concentration, transition or usability — is a separate question, which this architecture leaves open. Banks continue to issue and lend in their own denominated grassroots currencies beside every other issuer.

A run is on one issuer and is met from their holdings. The central bank can always meet presentations of its own sovereign coins by issuing fiat coins, so there is no open-ended digital run into central bank money.

Interest. With grassroots bonds [81], credit acquires time and a price. A bond is a unit of its issuer's debt due at a later date. Once the issuer's date reaches that date, its bearer may take a coin of the issuer for it. The discount at which coins are swapped for a bond, with its maturity, determines its rate of interest.

Every person can lend at interest, sell debt, open credit lines, post collateral, take deposits, and form the further financial instruments, each a swap of bonds or an escrow agreement. A bank's bond takes the place of its time deposit.

The central bank's instruments of monetary policy are the same operations, and it chooses the counterparty, amount, rate, maturity and collateral of its credit operations. The policy rate is the rate at which it lends its coins against bonds. Targeted liquidity is a term credit line to a city, a bank or a community, whose tranches are draws it consents to, each falling due at its maturity. It lends against escrowed collateral, and the lender of last resort [12] is such lending at a penalty rate to an issuer whose bonds cover their liabilities while their coins do not.

Interest is charged on the borrowing of sovereign grassroots coins and paid on the bonds the central bank issues to the counterparties it chooses; the coins bear none, as cash does not. A remunerated CBDC pays its rate to whoever holds it, and so competes with deposits, which is one reason neither the digital euro nor the digital pound is to be remunerated [18,46].

The central bank lends to a counterparty at one rate and pays another on the bonds it sells them. That counterparty will not pay more than the lending rate, since it can borrow from the central bank instead, and will not accept less than the bond rate, since it can buy a central bank bond instead. The two rates therefore bracket the rates it faces, at like maturity, collateral and risk. That bracket is the corridor [3], and the central bank chooses which counterparties it admits to it.

The retail CBDC proposals compared add a retail form of central bank money and leave the central bank's lending, its asset purchases and the implementation of the policy rate in reserves. In a sovereign grassroots currency they are transactions in the coins and bonds the public holds.

A central bank with sovereign grassroots currencies.

A central bank that issues sovereign grassroots currencies can therefore lend, absorb liquidity, set its rates and buy and sell securities in the coins and bonds the public holds, choosing the counterparties and terms of its credit operations, and without converting bank deposits into newly issued central bank money on demand.

What we show. We prove that one Dollar is the only arbitrage-free price of a Dollar-denominated grassroots coin whose issuer meets presentations, and argue that the central bank’s lending rate and the rate on its own bonds bound the rates its admitted counterparties face at like terms.

We verify sovereign grassroots coins against the three principles and fourteen features. We then compare them with the four CBDC architectures, the CBDCs in operation and in design, the system designs, and the private alternatives: who is the retail holder’s debtor, who keeps the retail record, who takes part in a payment, whether a payment can be made offline, who sees it, whether the central bank holds retail accounts, whether the central bank processes retail payments, who creates credit, what a payment costs, and how a lost key or device is recovered.

We also set sovereign grassroots coins, denominated grassroots coins and grassroots bonds among the types of money proposed as a CBDC or in its place—account-based CBDC, token-based CBDC, stablecoins and tokenised deposits—by whose liability each is, what backs it, its record, how it is created, whether it bears interest, and what can be done with it.

Status. The designs in operation have measured throughput, scale and ease of use; grassroots currencies run as a prototype [43,44,67] specified by a grassroots social contract [53,68], and have yet to be similarly measured.

Moreover, a digital economy of denominated grassroots currencies can form without the central bank of the denomination, spontaneously or by spilling over from a neighbouring economy, and the central bank can join it once formed by issuing its own denominated grassroots coins, which are then the sovereign ones.

2 Money: Sovereign Grassroots Coins

A sovereign grassroots coin is a digital debt of one unit of a fiat currency, issued by the central bank of that currency. Here we define it, describe how it enters and leaves circulation, and define its payment. It is the money of the architecture and the central bank digital currency proposed here; the credit of the persons is Section 4, and maturity and interest Section 5.

2.1 Denominated Grassroots Coins and Bonds

Persons, denominations and fiat coins. A *person* is natural or legal, with the gender-neutral pronoun “they”: a person, a household, a merchant, a cooperative,

a bank, a city, a government, a central bank. We assume a potentially infinite set of persons Π and consider only its finite subsets. Let $\mathcal{F}$ be a countable set of *denominations*, disjoint from Π , the identifiers of the fiat currencies (USD, EUR, KES, ...). A *fiat coin* is a unit of a fiat currency itself: cash, or a unit of central bank money on the central bank's conventional books, held by a person it admits to hold it; a sovereign grassroots coin is not a fiat coin. Anyone may hold cash, and reserves are held by the institutions the central bank admits, so the fiat coin a depositor is paid is cash, and their bank's reserves are the bank's own.

Bonds and coins. A grassroots coin is a unit of its issuer's debt, due now, backed by the issuer's offerings and by the coins and bonds they hold, and a grassroots bond is such a unit due at a later date [79,81]. The two are distinct instruments: a coin carries no date, and a bond is minted with a date later than its issuer's own. Here each carries a denomination and its obligation is a fixed sum of it.

Definition 2.1 (Denominated Grassroots Coin and Bond). *An f -denominated grassroots p -coin, denoted $\mathfrak{c}_{f,p}$, is a unit of debt of the currency $f \in \mathcal{F}$ issued by the person $p \in \Pi$, due now. An f -denominated grassroots p -bond with maturity date d , denoted $\mathfrak{c}_{f,p,d}$, is such a unit due at the date $d \in \mathbb{N}$. The f -denominated grassroots currency of p consists of the f -denominated p -coins and p -bonds. We write $\mathfrak{c}_{f,p}^k$ and $\mathfrak{c}_{f,p,d}^k$ for multisets of k of each. Amounts are in the smallest unit of f , so every count is an integer.*

Holdings and dates. Each person holds a multiset of coins and bonds and keeps their own calendar; d_p^* denotes the local current date of p , advanced by the calendar, and there is no global clock. A bond is minted with a date later than its issuer's own, so no bond is born due. A bond $\mathfrak{c}_{f,q,d}$ is *mature* iff $d \leq d_q^*$, and its bearer may then take a q -coin for it, at their own election: maturity is judged by the date of the issuer and the dates of the holders play no part [81]. A coin carries no date, so no advance of an issuer's date makes or unmakes one.

The obligations. An f -denominated grassroots p -coin is a promissory note signed by p , stating its issuer and denomination, and a p -bond states a maturity date besides. Each carries three obligations:

1. p prices their offerings in their own f -denominated coins and accepts them in payment at those prices;
2. p prices every f -denominated coin and bond they hold at par against their own f -denominated coins, on standing offer; and
3. an f -denominated grassroots coin is a debt of one unit of f , intended to be legally binding under the applicable law (Section 2.4), and its bearer may present it to its issuer, who must redeem it at face value; a p -bond is the same debt due at its date, and once mature its bearer may take a p -coin for it.

The issuer fulfils a presentation by an f -denominated coin or bond they hold, of the bearer's choice — set-off, when the instrument taken is the bearer's own — or by a fiat coin, performed outside the operations of the currency and legally

enforceable. A bearer may take a bond rather than a coin: a debt due later of a person they trust can be worth more to them than a debt due now of one they trust less. A presentation left unfulfilled evidences the issuer's default in f . The issuer assumed the three obligations voluntarily, by minting the coin or bond, and declining a payment or a presentation is a breach of its terms, actionable at law where the obligation is enforceable (Section 2.4).

The transactions. A person mints coins of their own, of any denomination, and bonds of any later maturity, at their own election; two persons swap coins and bonds of one denomination, by a transaction of both; a person accepts in payment, up to a limit of their own setting, the coins of an issuer whose coin or bond they hold; a holder pays the payee coins the payee accepts — the payee's own, the payer's own, or those of a third person, who takes part in the payment; the bearer of a coin presents it to its issuer and takes for it any coin or bond of that denomination the issuer holds, and the bearer of a matured bond takes a coin of its issuer; and a person may deposit coins or bonds with an escrow agent for a third person, who releases them or returns them as the agreed condition is met or fails. These are the transactions of the grassroots social contract of Appendix A: the contract of grassroots currencies [79], with the dates and the escrow of grassroots bonds [81], with denomination, and with the acceptance of named currencies in payment, which the contract of grassroots currencies leaves to an extension [79]. A swap in which each party gives coins of their own issue opens a mutual credit line; one in which a party gives coins and the other their own bonds of larger face value maturing later is a loan.

The clauses compile to volition-guarded multiagent atomic transactions [53, 68], which we recall from [79,81] with the denomination and the acceptances added. Each agent is a person operating a machine, and the machine state of a person p is their holdings c_p , a multiset of coins and bonds, initially empty; their date d_p^* , initially 0; the warranties w_p they have received, a set of pairs of an issuer and a date, initially empty; and the acceptances A_p they have granted, a multiset of pairs of an issuer and a denomination, initially empty. A *configuration* c records the state of every person. A transaction changes the machine states of its participants and no one else's, is enabled when its precondition holds, and is *guarded* by the persons among its participants whose consent it takes: it is taken only when every guard is willing. A run is *safe* if every step is a transaction of the protocol, *live* if a class of equivalent transactions that is enabled and willed by its guards is eventually taken, and *correct* if it is both; a protocol is *volitionally grassroots* if any group of persons may operate it on its own, and two groups become connected only by a transaction willed by a member of each [68]. Multiset sum and difference are written $\uplus$ and $\setminus$.

Definition 2.2 (The Transactions of Denominated Grassroots Currencies). *For persons $p \neq q \in \Pi$, $e \in \Pi$ distinct from p and q , $u, v, r \in \Pi$, a denomination $f \in \mathcal{F}$, maturity dates $d, d' \in \mathbb{N}$, a date $t \in \mathbb{N}$, amounts $k, k' \geq 1$, and a limit $L \geq 1$, the **transactions of denominated grassroots currencies** are the volition-guarded transactions $(c \rightarrow c', Q')$ below, over the participants named, in which c satisfies the precondition stated and every component of a*

participant's state not named is unchanged. We write $\phi_{f,u,*}^k$ for k instruments of u in f of one kind and maturity, coins or bonds, where the transaction does not distinguish them:

1. **Mint** _{p} (f, k) and **Mint** _{p} (f, d, k), over $\{p\}$, guarded by $\{p\}$: the second with precondition $d > d_p^*$, so no bond is born due; $c'_p = c_p \uplus \phi_{f,p}^k$ and $c'_p = c_p \uplus \phi_{f,p,d}^k$ respectively.
2. **Advance** _{p} (t), over $\{p\}$, guarded by $\emptyset$: precondition $t > d_p^*$; $d'_p = t$.
3. **Swap** _{p,q} ($\phi_{f,u,*}^k, \phi_{f,v,*}^{k'}$), over $\{p, q\}$, guarded by $\{p, q\}$: precondition $\phi_{f,u,*}^k \subseteq c_p$ and $\phi_{f,v,*}^{k'} \subseteq c_q$; $c'_p = c_p \setminus \phi_{f,u,*}^k \uplus \phi_{f,v,*}^{k'}$ and $c'_q = c_q \setminus \phi_{f,v,*}^{k'} \uplus \phi_{f,u,*}^k$.
4. **Accept** _{p} (f, u, L), over $\{p\}$, guarded by $\{p\}$: precondition $\phi_{f,u,*} \in c_p$; $A'_p = A_p \uplus L \cdot \{(u, f)\}$.
5. **Pay** _{p,q} ($\phi_{f,u}^k$), over $\{p, q, u\}$, guarded by $\{p\}$: precondition $\phi_{f,u}^k \subseteq c_p$ and $u = q$ or $k \cdot \{(u, f)\} \subseteq A_q$; $c'_p = c_p \setminus \phi_{f,u}^k$, $c'_q = c_q \uplus \phi_{f,u}^k$, and $A'_q = A_q \setminus k \cdot \{(u, f)\}$ if $u \neq q$. Only coins are paid.
6. **Redeem** _{p,q} ($f; r, *$), over $\{p, q\}$, guarded by $\{p\}$: precondition $\phi_{f,q} \in c_p$ and $\phi_{f,r,*} \in c_q$; $c'_p = c_p \setminus \phi_{f,q} \uplus \phi_{f,r,*}$ and $c'_q = c_q \setminus \phi_{f,r,*} \uplus \phi_{f,q}$. The bearer takes a coin or a bond, at their own choice.
7. **Mature** _{p,q} (f, d), over $\{p, q\}$, guarded by $\{p\}$: precondition $\phi_{f,q,d} \in c_p$ and $d \leq d_q^*$; $c'_p = c_p \setminus \phi_{f,q,d} \uplus \phi_{f,q}$ and $w'_p = w_p \cup \{(q, d_q^*)\}$. The bearer of a matured bond takes a coin of its issuer, at their own election.
8. **Deposit** _{p,e} ($\phi_{f,u,*}^k$), over $\{p, e\}$, guarded by $\{p, e\}$: precondition $\phi_{f,u,*}^k \subseteq c_p$; $c'_p = c_p \setminus \phi_{f,u,*}^k$ and $c'_e = c_e \uplus \phi_{f,u,*}^k$.
9. **Release** _{e,q} ($\phi_{f,u,*}^k$) and **Return** _{e,p} ($\phi_{f,u,*}^k$), over $\{e, q\}$ and $\{e, p\}$, guarded by both participants: precondition $\phi_{f,u,*}^k \subseteq c_e$; the instruments are deleted at e and added at the other participant.

Two transactions are **equivalent** iff they have the same name and arguments, differing only in the configurations c and c' .

Each is a schema of Appendix A at a binding: the participants are the roles, the guards are the guarding roles, the precondition collects what the roles require, and the effect collects what they add and delete; Pay is three schemas, with the issuer u the payee, the payer, or a third role. Mint, accept, pay, redeem and mature are guarded by the initiator, a swap and each escrow transfer by both parties, and advance-date by no one, as local time advances mechanically; the issuer of the coins paid is a participant of every payment in their coins and not a guard of it. Denomination adds the argument f to every transaction of grassroots bonds and changes no guard. Acceptance is a quota and not a cap on exposure: **Accept** _{p} (f, u, L) grants L , each u -coin paid to p uses one, and p may grant again, so p consents in advance, and in a bounded quantity, to every rise in their exposure to u ; the per-issuer limit of grassroots currencies [79] bounds the exposure itself.

Lemma 2.3 (Conservation of Debt [68,79,81]). *In any safe run, the f -denominated debts of p in any configuration are exactly those p minted in the prefix of the run ending in it, each of them a p -coin or a p -bond of one unit of f .*

Proof. Mint adds new debts of p at p ; swap, pay, redeem, deposit, release and return move instruments between participants without creating or destroying them; mature replaces a matured p -bond by a p -coin, the same debtor and the same face value; advance and accept change no holding.

Corollary 2.4 (No Cross-Denomination Transactions). *Every transaction of an f -denominated grassroots currency is over f -denominated coins and bonds.*

Proof. Every act schema of the contract carries one denomination variable, which every atom of the schema carries (Appendix A), so no binding of any schema moves instruments of two denominations.

Denomination requires no permission from the central bank of the denomination: a person may issue bonds of several denominations at once, as denominating a private debt in dollars requires no permission from the Federal Reserve. Issuing instruments that circulate in payment may engage banking, electronic-money, securities, money-transmission and consumer-protection law, which is a matter of each jurisdiction. A denominated grassroots currency therefore operates before and without the sovereign of its denomination, on the obligations of its issuers, and the sovereign may join it once it is formed (Section 2.2).

2.2 The Sovereign

Each fiat denomination has a sovereign issuer, or *sovereign*: the central bank of the currency. We assume a total function $\sigma : \mathcal{F} \rightarrow \Pi$ that maps a denomination $f \in \mathcal{F}$, say the Dollar, to its sovereign, written $f_\sigma \in \Pi$, say the central bank of the Dollar.

Definition 2.5 (Sovereign Grassroots Currency). *The **sovereign grassroots currency** of $f \in \mathcal{F}$ is the f -denominated grassroots currency of the sovereign f_σ . Its coins are the **sovereign grassroots coins** of f , and its bonds the **sovereign grassroots bonds** of f .*

A grassroots currency comprises the coins and the bonds of its issuer, and the central bank digital currency proposed here is the sovereign grassroots coins. The sovereign bears the obligations of Definition 2.1 as every issuer does, and only it can issue a fiat coin to fulfil a presentation of its own coins. It is otherwise an ordinary party: it mints, swaps, accepts, pays and redeems by the same transactions, the contract does not name it (Appendix A), and it may join a denominated grassroots currency already in operation as one more issuer.

2.3 Issuance and Redemption

The obligation runs one way. Redemption is the return of a coin to its issuer, and it is obligatory: the bearer presents the coin at their own election and the issuer is bound to fulfil the presentation (obligation 3). Issuance is minting together with a swap or a payment, and both are transactions the issuer takes at

their own election: no obligation requires an issuer to mint, or to part with what they have minted. The debts of an issuer in circulation, coins and bonds together, therefore grow only by transactions the issuer consents to, and redemption only reduces them (Lemma 2.3). Maturity moves face value from the issuer's bonds to their coins, at the bearer's election, and adds no debt: the bearer takes a coin for a bond the issuer had already minted and parted with.

How sovereign grassroots coins enter circulation. The central bank mints its coins and parts with them by a swap or a payment: it swaps them for fiat coins presented to it, and it pays them out to persons who accept them (Definition 2.2). It need not swap them for bank deposits on demand, and here it does not: no guaranteed on-demand convertibility of bank deposits into the central bank digital currency is one of Kumhof and Noone's four principles [65]. The central bank holds no retail account, and a person who holds no sovereign grassroots coin obtains one from the central bank against a fiat coin, or from a person who holds one, by payment, by swap or by redemption. Buying and selling bonds and other securities for its coins belongs to the third component, where it is an open market operation (Section 5.3).

How they leave circulation. On presentation the central bank fulfils by a fiat coin, which it issues, or by any f -denominated coin or bond it holds. Fulfilling by a fiat coin is performed outside the contract, and its effect within the currency is the payment of the coin to its issuer, a transaction of Definition 2.2, so Lemma 2.3 covers it. Redemption into fiat coins reduces the sovereign grassroots coins in circulation, and no demand for conversion increases them. The sovereign grassroots coins and bonds in circulation are therefore bounded by what the central bank has issued and not taken back, and maturity moves face value from its bonds to its coins and adds nothing to the two together (Lemma 2.3). What an issuer has *issued* is what they have minted and parted with, coin or bond, here and below.

A direct central bank digital currency. Retail designs are classified by who holds the retail claim and who keeps the retail record [8,10]. By that classification sovereign grassroots coins are a direct central bank digital currency: the public holds a claim on the central bank and on no intermediary, the central bank takes part in every payment in its coins, and no intermediary keeps a retail record. The central bank keeps a log of the transactions in its coins rather than a table of balances by identity, and that log determines who holds each coin, so it serves as the retail record of the classification. They differ in the machinery from the direct designs in which the central bank keeps every retail balance and executes every retail payment on its own ledger [18,45,69]: each person keeps their own holdings, the central bank keeps the record of its own coins, a payment is disseminated over the social graph [67], and it is final when the central bank has countersigned it, with no consensus.

What the money component does not do. The coins create no credit and open no lending channel for the central bank, and they add no instrument of policy: remuneration and limits on holdings can be added, as in the other designs,

and are not part of them. Credit is the second component (Section 4) and interest the third (Section 5).

2.4 A Payment and Its Digital Realisation

The realisation is that of grassroots currencies [67,79]: a coin is a digitally signed promissory note, the identity of a person is their signature key, and the issuer, a party to every payment in their coins (Definition 2.2), countersigns every transaction in their own currency and may not withhold the countersignature from one the contract permits. Every transaction is volition-guarded and multiagent atomic [53,68], and denomination restricts the bonds of a transaction to one denomination (Corollary 2.4) and changes neither the transactions nor their guards.

A payment. A payment is a signed message from the payer to the payee, countersigned by the issuer of the coins paid and recorded in the issuer’s log. The countersignature proves holdership and prevents double spending [67]. The log is held by machines the issuer designates: for a natural person, state custodians chosen among their friends [44]; for an institution, its own machines. A payment is final when the issuer has countersigned it and the machines holding the issuer’s log have recorded it: no shared ledger is updated, no block is awaited, and no third party agrees.

Who takes part, and who sees. A payment needs its payer, its payee, the issuer of the coins paid and those machines. It is confidential to the three parties: the persons of the custodians have no access to the log their machines hold [44], and there is no shared ledger, no operator and no intermediary. A payment in sovereign grassroots coins therefore proceeds over any network that reaches the central bank and the machines holding its log, and not offline from them, and the central bank sees it. The central bank does not see a payment in the coins of another issuer unless it is itself a party to it.

Cost and throughput. No intermediary takes part, so the architecture requires no fee, and the cost to a person is that of operating their device; an issuer is free to charge for their services. The throughput of payments in sovereign grassroots coins is bounded by the central bank and by the machines holding its log, as in a direct central bank digital currency.

The legal instrument. A denominated grassroots coin is a cryptographically signed debt instrument, and its issuer is identified by their signature key. In the United States a signature, contract or record may not be denied legal effect, validity or enforceability solely because it is in electronic form [86]; in the European Union an electronic signature shall not be denied legal effect and admissibility as evidence solely on the grounds that it is in electronic form [47]; and the UNCITRAL-model acts say the same where they are adopted [83]. Three propositions are distinct, and only the first follows from those statutes: that the record is admissible and not denied effect for being electronic; that the obligation it states — one unit of its fiat currency (Definition 2.1) — is an enforceable

debt of its issuer, which rests on the ordinary rules of contract and on the jurisdiction; and that the instrument is a negotiable note within the bills and notes acts [7,66,84], which it does not claim. A denominated grassroots bond is analogous to a promissory note, and closer to one than an undenominated grassroots coin [79]: it promises a sum certain in money at a date certain, which those acts require and the undenominated coin lacked. Whether it is one within them is a question for each jurisdiction, open because the promise is surrounded by the other undertakings of Definition 2.1 and because a presentation may be fulfilled in kind. The protocol records the provenance of each coin and prevents its double spending, serving the purpose that the rules of transfer and of proof of holdership serve for paper notes. The UNCITRAL Model Law on Electronic Transferable Records [85] addresses this directly. Where it is enacted, an electronic record is the functional equivalent of a transferable document or instrument if a reliable method identifies it as that record, keeps it capable of being subject to control, and retains its integrity, and the requirement of possession is met by exclusive control, identified with the person in control. Whether the protocol's signatures, log and countersignature are such a method, and whether the Model Law is in force, are questions for each jurisdiction. The Model Law is technology-neutral and does not alter the substantive law of the instrument. The authority of a central bank to issue this liability is a fourth proposition, statutory and jurisdiction-specific: the Bank of England states that a digital pound would be introduced only once Parliament had passed the primary legislation for it [17]. The central bank's mandate we take as given.

Recovery of a lost key or device. A person who loses their key or their device recovers their identity from their identity custodians and their log, exactly, from their state custodians, and resumes without double spending [44]. An institution recovers its log from its own machines.

Status. Grassroots Flash [67] is a protocol with proofs of safety, liveness and the grassroots property; recovery from the loss of a key or a machine is specified and proved in [44]. The transactions of Definition 2.2 are abstract; a program is an executable realisation of them among parties who run it; and the secure coins of [44] are a third level, in which the issuer signs every transaction in their coins and state custodians hold copies of the log: that paper implements them by communicating volitional agents and proves that the implementation realises the specification at quiescence, conserves money, recovers the log exactly after the loss of a key or a machine, never double-spends after recovery, and finalises a requested payment while the issuer and a supermajority of its custodians stay live. The transactions of the currency have a prototype implementation in GLP [80,81], with grassroots currencies running as a certified mini-app of the Grassroots Super-App on a physical smartphone [43,79]; the denominated agent is a certified mini-app too, since GLP `a6bac767`, and the bond agent it is derived from keeps a network entry and is not certified. The denominated agent implements eight of the nine transactions it shares with grassroots bonds, with the denomination as the coin's middle argument; mature, accept, payout and spend are not yet implemented. The program also lags the two instruments of

Definition 2.1: it has no separate coin, representing one as a bond of maturity 0, and it gives the date warranty in every payment and redemption rather than when a matured bond is taken for a coin. The two extensions are separate: denomination adds the argument f to every transaction of grassroots bonds and adds no transaction, while the acceptance of named currencies in payment, which the contract of grassroots currencies leaves to an extension [79], adds the three transactions accept, payout and spend (Appendix A). The operations of the sovereign are the same operations, performed by the sovereign. The denominated transactions run as a separate program, derived from the bond agent: the village market of [81] denominated in one fiat currency, with the central bank as an eighth party that mints sovereign grassroots coins and opens a mutual credit line with the community bank by a swap of coins for coins, a chain redemption that leaves a household holding a sovereign grassroots coin, and the central bank settling the presentation of that coin in the fiat currency itself. The central bank runs the same agent, and the contract does not name it. Denomination itself changed no message type and no step of the protocol; the argument itself reached every line that names a bond, and the fulfilment of a presentation by a unit of the fiat currency, which the contract leaves outside itself, is separate code.

3 Sovereign Grassroots Coins as a Central Bank Digital Currency

Seven central banks and the Bank for International Settlements have stated what a retail central bank digital currency must satisfy [14]: three foundational principles — do no harm to monetary and financial stability, coexistence with cash and other forms of money, and innovation and efficiency — and fourteen core features in three groups. The instrument features are convertibility at par, convenience, acceptance and availability including offline, and low or no cost to end users; the system features are security, instant settlement, resilience, continuous availability, high throughput, scalability, interoperability and flexibility; the institutional features are a robust legal framework and conformity with regulatory standards. The same group has analysed the financial-stability implications of a central bank digital currency [15] and its system design [16].

Tables 1 and 2 check sovereign grassroots coins against the three principles and the fourteen features, naming for each the mechanism of Section 2 it rests on and its status. The coins are checked by themselves, before the credit of the persons and the bonds; where a later component strengthens a row, the cell names its section. The paragraphs below add what a cell cannot hold.

Disintermediation. Deposits converted into central bank money leave the banks to fund themselves in wholesale markets, at higher cost and less stably, and to lend less or at higher rates [15]. The mitigants proposed are limits on holdings, limits on transactions, no or tiered remuneration, and a waterfall that sweeps holdings above a limit into a bank account [15]; the digital euro adopts non-remuneration, a holding limit and a reverse waterfall that draws on a linked

bank account [46]. Each of them caps the central bank digital currency a person may hold, and each is needed because the design converts deposits into it on demand. Here the obligation runs one way (Section 2.3): the central bank is bound to redeem its coins and is bound to issue them to no one, so the public holds what the central bank has issued and not taken back, coins and bonds together. No operation turns a bank deposit into newly issued central bank money on demand: no holder of a bank deposit has a right to newly issued sovereign grassroots coins, and a bank's reserves are the bank's own, so a depositor obtains sovereign grassroots coins from a holder, which reallocates coins already in circulation, or from the central bank against cash their bank pays them, where the central bank elects to make that exchange — which changes the form of central bank money and not its quantity (Lemma 2.3). Here the central bank's issuance does what the mitigants do from outside, and no limit, tier or waterfall is added to bound the demand-driven creation of central bank money; whether one is wanted for concentration, transition or usability is a separate question, which this architecture leaves open.

Runs. A run into central bank money costs less than a run into cash, so a systemic run may be faster and larger; how much so depends on the design of the central bank digital currency and on the credibility of deposit insurance [15]. A run reaches sovereign grassroots coins only through the holders of them, and the central bank can always fulfil a presentation of its own coins by issuing a fiat coin, so no presentation goes unmet and no run creates a debt of the central bank. What the public can obtain of them is bounded by what the central bank has issued and not taken back, coins and bonds together, and maturity turns one of its bonds into one of its coins and creates no debt of it. So a run on a bank is bounded by what that bank can pay its depositors, as it is today, and no run brings newly issued central bank money into being.

Offline payment. A payment in sovereign grassroots coins needs the central bank and the machines holding its log to be reachable (Section 2.4), so it cannot be made offline from them, and the feature is not met. The reports reach offline payment through the risk-taking of intermediaries [8] or through value stored on the device [45]; neither is adopted here. A payment in the coins of a person who is present proceeds over a local network with no connection to the Internet, which is the second component (Section 4); it is not offline from that issuer either.

Conformity with regulatory standards. Full anonymity is not plausible for a central bank digital currency, which must meet the requirements against money laundering and the financing of terrorism [14,16]. Identities here are key-pairs, and the central bank's log records every payment in its own coins and the counterparty of every transaction it takes, so that log is a complete transaction trail by protocol identity. A key identifies a party to the protocol and not, by itself, a verified natural or legal person: binding the two, and applying the know-your-customer, anti-money-laundering and record-keeping rules to the party so identified, is a function of the deployment and its jurisdiction, as it is today.

What the list does not ask for. The fourteen features ask what the money is and how it is paid; none asks who creates credit, and none asks whether

the central bank’s instruments of policy operate in the instrument the public holds. Sovereign grassroots coins are checked against the list and leave credit creation and the operations of monetary policy where every other design leaves them, in bank money and central bank reserves. That is the second limitation of Section 1, and the two components that follow answer it: the credit of the persons (Section 4), and maturity and interest (Section 5).

Table 1: The three foundational principles of a retail central bank digital currency [14] against sovereign grassroots coins: the mechanism each rests on and its status. The coins are checked by themselves, before the credit of the persons (Section 4) and the bonds (Section 5); a cell names a later section where that component strengthens the row. “By construction” is claimed for what the architecture fixes, “argued” for what rests on an argument under stated assumptions.

Requirement [14]	How sovereign grassroots coins meet it	Status
1. Foundational principles		
<i>1.a Do no harm: disintermediation</i>	No retail account, and no conversion of a bank deposit on demand [65]: the central bank issues its coins in exchange for fiat coins and by its own payments, so no deposit becomes newly issued central bank money; with the credit component it issues them by mutual credit lines (Section 4)	argued
<i>1.b Do no harm: runs</i>	The central bank can always fulfil a presentation of its own coins by issuing a fiat coin, and what the public can obtain of them by redemption is bounded by what it has issued, so there is no open-ended digital run into central bank money	argued
<i>1.c Do no harm: monetary policy</i>	The coins bear no interest, as cash does not, so they introduce no interest-rate competition with deposits, and policy is conducted as it is today; with the bonds the policy rate becomes the rate at which the central bank lends its coins (Section 5)	argued
<i>1.d Coexistence</i>	Redeemable at face value for a unit of the fiat currency by the central bank’s obligation (obligation 3); cash and bank money continue; the central bank joins a non-sovereign grassroots currency already in operation as one more issuer	by construction
<i>1.e Innovation and efficiency</i>	A payment needs no infrastructure beyond the parties’ devices and the machines holding the issuer’s log; every person may issue a currency of their own beside the central bank’s (Section 4)	by construction

Table 2: The fourteen core features of a retail central bank digital currency [14] against sovereign grassroots coins, as Table 1.

Requirement [14]	How sovereign grassroots coins meet it	Status
2. Instrument features		
<i>2.a Convertible at par</i>	Redeemable by the central bank for one unit of the fiat currency, which it issues (obligation 3)	by construction
<i>2.b Convenient</i>	A payment is a signed message countersigned by the central bank, on the parties' own devices; no account beyond a keypair; ease of use unmeasured	specified
<i>2.c Accepted and available, offline included</i>	Acceptance by the central bank is enforced by the contract; a payment needs the payer, the payee, the central bank and the machines holding its log, so it proceeds over any network that reaches them, and not offline from the central bank	not met
<i>2.d Low or no cost to end users</i>	No intermediary, so no fee is required by the architecture; what a person pays is the cost of operating their device, and what an issuer charges for its services, neither measured	by construction; cost unmeasured
3. System features		
<i>3.a Secure</i>	The central bank countersigns every payment in its coins, proving holdership and excluding double spending; a holder who loses their key or device recovers their identity from their identity custodians and their sovereign grassroots coins from the central bank's log [44]; these are properties of the protocol, and the resistance of a deployment to attack is not established by them	proved; to be deployed
<i>3.b Instant settlement</i>	Final when the central bank has countersigned it and the machines holding its log have recorded it: no consensus and no intermediary; the time this takes is that of the network and the machines	by construction; latency unmeasured
<i>3.c Resilient</i>	Payments in sovereign grassroots coins need the central bank and the machines holding its log, and no other component; a holder's loss of key or device is remedied from their custodians [44]	specified
<i>3.d Continuously available</i>	No opening hours and no maintenance window; the availability of the coins is that of the central bank and of the machines holding its log	specified
<i>3.e High throughput, scalable</i>	The central bank and the machines holding its log bound the throughput of payments in its coins, as in a direct central bank digital currency; the currencies of the persons add throughput of their own (Section 4)	unmeasured

continued on the next page

Requirement	How sovereign grassroots coins meet it	Status
<i>3.f Interoperable</i>	Meets the existing systems at redemption, into central bank money or a fiat coin through the banking tools of the currency; exchange across denominations by escrow (Appendix D)	specified; to be deployed
<i>3.g Flexible and adaptable</i>	Instruments are swaps and escrow agreements under conditions; a new instrument is a new condition, with no change to the contract (Section 5)	by construction; to be deployed
4. Institutional features		
<i>4.a Robust legal framework</i>	Three distinct propositions: the signed record is not denied legal effect for being electronic [47,86]; the obligation it states is an enforceable debt of the central bank of one unit of the fiat currency, which rests on the ordinary rules of contract and on the jurisdiction; and the central bank's authority to issue this liability is statutory, the digital pound to be introduced only once Parliament has passed the primary legislation [17]. The mandate this paper takes as given	argued
<i>4.b Conformity with regulatory standards</i>	The central bank's log records every payment in its coins and the counterparty of every transaction it takes, a complete trail by protocol identity, which supports know-your-customer, anti-money-laundering and record-keeping requirements; binding a key to a verified legal person, and conformity itself, are the deployment's and the jurisdiction's	argued

4 Credit and Liquidity: Non-Sovereign Grassroots Coins

Every person, natural or legal, issues an f -denominated grassroots currency of their own (Definition 2.1), on the same three obligations the central bank bears. Here we add them to the money of Section 2: what their credit is and how it is created, how the central bank issues its coins against theirs, why a coin of theirs is worth one unit of the fiat currency, and what a run on one of them reaches. With them, sovereign grassroots coins are the base money of the denomination.

4.1 Every Person an Issuer

Credit by mutual credit. Two persons open a mutual credit line by swapping coins of their own issue: each thereafter holds coins of the other, and each may pay the other in the other's coins or present them for redemption. The credit so created is inside money [30,72], secured by social collateral [20]: the borrower's standing in their community, the acceptance of their currency, and the mutual credit lines they hold. Default costs the issuer that standing — an unfulfilled presentation evidences it, holders redeem what the issuer still holds, and no one

extends them new credit [20,79]. Credit is thus created by every person, which none of the designs compared allows, and a bank's coins play the economic role of its demand deposits.

Who pays in what. Households, firms and banks accept payments in their own currencies, in the currency of the bank they are customers of, or in the sovereign grassroots currency (Definition 2.2). The central bank holds no retail account and takes part in no payment but in its own coins, to every one of which it is a party (Definition 2.2). Banks settle among themselves by set-off and by chain redemption (Section 4.3), and need no central bank money to do so.

A payment in the coins of a person. The payment of Section 2.4 is the same transaction with another issuer: signed by the payer, countersigned by the issuer of the coins paid, recorded in the issuer's log by the machines holding it. It needs its payer, its payee, the issuer and those machines, so it proceeds over any network that reaches them — Bluetooth, or a local network with no connection to the Internet — and it is confidential to the three parties. No component is shared by all issuers, so none bounds the throughput of the whole, which grows with the issuers and their custodians. The central bank does not see these payments unless it is itself a party to one.

4.2 The Central Bank's Mutual Credit Lines

Issuance against the counterparty's coins. A counterparty who issues coins of their own gives the central bank something to lend against. Here the central bank issues its coins by mutual credit lines, and guarantees no conversion of bank deposits into them on demand. A mutual credit line is a swap of its coins for the coins of the counterparty it chooses — a bank, a city, a firm, a cooperative or a household, any counterparty the architecture admits and its mandate allows — in the amount and at the time it chooses, with no bank between them and no account at the central bank. The counterparty's coins are redeemable against their holdings, and their coins in circulation are redeemable in full exactly when their holdings cover them (Section 4.4) [79].

The precedent, and the difference. Issuance that is not by conversion is Kumhof and Noone's principle [65]: no guaranteed on-demand convertibility of bank deposits into the central bank digital currency, and issuance only against eligible securities, principally government securities. There the central bank buys securities its counterparty already holds; here it lends against coins its counterparty issues. The counterparty of an asset purchase is whoever holds the security; the counterparty of a mutual credit line is whoever the central bank chooses. We adopt that principle and not their separation of the currency from reserves: a sovereign grassroots coin is redeemed into a fiat coin on presentation, without restriction (Definition 2.1), and the quantity is governed by issuance rather than by a bar on convertibility. A mutual credit line is at par, on demand and without interest; the term credit line of Section 5.2, an escrowed facility whose draws carry maturities and interest, belongs to the third component [81].

Creation and the quantity of base money. As the central bank's lending creates reserves today, its mutual credit lines create sovereign grassroots coins, and unlike reserves the public holds and pays them. The sovereign grassroots coins and bonds in circulation are at most what the central bank has issued and not taken back (Section 2.3): they enter circulation only by transactions of the central bank, and thereafter circulate by payment, swap and redemption, redemption into fiat coins reducing them and no demand of a depositor increasing them. Maturity moves face value from its bonds to its coins and adds nothing to the two together.

Quantity and allocation, and no rate. A swap of coins is at par, on demand and bears no interest, so what the central bank sets by a mutual credit line is the counterparty, the quantity and the timing of the liquidity it provides, and not a rate. The rate arrives with maturity (Section 5). Every other person creates credit independently of the central bank, by their own mutual credit lines.

Disintermediation and runs. Sovereign grassroots currencies add no on-demand operation that turns a bank deposit into newly issued central bank money: no holder of a bank deposit has a right to newly issued sovereign grassroots coins, and a bank's reserves are the bank's own. A depositor obtains sovereign grassroots coins from a holder, which reallocates coins already in circulation, or from the central bank against cash their bank pays them, where the central bank elects to make that exchange, which changes the form of central bank money and not its quantity (Lemma 2.3). No limit, tier or waterfall is therefore needed to bound the demand-driven creation of central bank money, which the central bank issues at its own election; whether a limit is wanted for other reasons — concentration, transition or usability — is a separate question, which this architecture leaves open; the Bank of England has measured what a limit is worth where deposits are converted on demand [37]. Banks continue to issue and to lend in their own grassroots currencies beside every other issuer. A run is a run on one issuer and is met from their holdings (Section 4.4). The central bank can always meet presentations of its own coins by issuing fiat coins, and what the public can obtain of them by redemption is bounded by what it has issued, so there is no open-ended digital run into central bank money.

4.3 The Peg and the Price of a Coin

Redemption reaches across chains of holdings, coin by coin.

Proposition 4.1 (Chain Redemption [79,81]). *Let $p_0, p_1, \dots, p_k$ be a sequence of distinct persons with $k \geq 1$ such that each p_i , $0 \leq i < k$, holds an f -denominated p_{i+1} -coin. Then from that configuration there is a sequence of $k - 1$ redemptions by p_0 whose effect is that p_0 holds an f -denominated p_k -coin.*

Definition 4.2 (f -Holding Graph, Sink, Sovereign-Connected). *Given a configuration, the f -holding graph is the directed multigraph with the persons as vertices and an edge $u \rightarrow v$ for each f -denominated v -coin and each f -denominated v -bond that person $u \neq v$ holds; its **sink** is the sovereign f_σ ; and*

the *f*-coin holding graph is its subgraph of the edges of coins. A person p is **sovereign-connected in f** if the *f*-coin holding graph has a directed path from p to f_σ .

The out-degree and in-degree of p in the *f*-holding graph are their assets a_p and liabilities ℓ_p in f , counted in coins and bonds [79,81]; a coin or bond an issuer holds of their own carries no value and no edge. A directed path from p to q in the *f*-coin holding graph is a chain of mutual liquidity: by Proposition 4.1, after a sequence of redemptions along it p holds an *f*-denominated q -coin, and the coins along it are consumed. In particular f_σ is sovereign-connected in f , by the empty path.

Proposition 4.3 (Peg Propagation). *Let q hold an f -denominated p -coin, where p is sovereign-connected in f . Then there is a sequence of redemptions by q , in the denomination f , whose effect is that q holds a sovereign grassroots coin.*

Proof. q holding an *f*-denominated p -coin is an edge $q \rightarrow p$ of the *f*-coin holding graph, and p being sovereign-connected in f is a directed path from p to the sovereign, so the graph has a directed path from q to f_σ , and with it a simple such path, whose persons are distinct and each of which holds an *f*-denominated coin of the next. By Proposition 4.1, after a sequence of redemptions along it q holds an *f*-denominated coin of the sovereign.

The two legs of the peg. The *direct leg* is the issuer's obligation (Definition 2.1): an *f*-denominated grassroots coin is a claim of one unit of f on its issuer, worth the issuer's credit, fulfilled in kind or by a fiat coin. The *mechanised leg* is Proposition 4.3: for a sovereign-connected issuer, redemption within the currency realises the claim in the sovereign's base money, whatever fiat the issuer holds. A person's coins trade at par with the unit of f while they meet redemptions as these arrive, and their capacity to meet them is measured by the ratios of Section 4.4. Proposition 4.3 moves one coin and consumes the coins along its chain, so being sovereign-connected secures the price of a coin and not the volume redeemable at once; what a group can obtain now is the maximum flow of Section 4.4.

The price of a coin. Arbitrage makes par the price of the coins of an issuer who meets presentations, whether by fiat coins or by coins of issuers who meet theirs. The persons who meet presentations in f are defined in stages: those who fulfil every presentation by a fiat coin, then those who fulfil every presentation by a fiat coin or by a coin of a person of an earlier stage.

Definition 4.4 (Meeting Presentations). *Let M_f^0 be the set of persons who fulfil every presentation of their f -denominated coins by a fiat coin, and M_f^{k+1} the set of persons who fulfil every such presentation by a fiat coin or by an f -denominated coin of a person in M_f^k . A person **meets presentations in f** if they belong to $M_f = \bigcup_k M_f^k$.*

The argument that follows is the model's, and frictionless: a swap or a redemption costs nothing, the obligations of Definition 2.1 are met as assumed, newly minted coins can be sold at the quoted price while that price stands, and the arbitrage itself does not exhaust the issuer's capacity to meet presentations.

Proposition 4.5 (Par by Arbitrage). *Let p meet presentations in f . Then one unit of f is the only arbitrage-free price of an f -denominated p -coin.*

Proof. Suppose an f -denominated p -coin trades at $\pi < 1$ units of f . A buyer acquires one and presents it to p , receiving a fiat coin or a coin of a person of an earlier stage, which they present in turn; with $p \in M_f^k$, at most $k + 1$ presentations end in a fiat coin, one unit of f for π : a gain of $1 - \pi$ per coin, without risk, repeated while the price stands. Suppose it trades at $\pi > 1$. Minting costs p nothing and obliges them for one unit of f per coin (Definition 2.1), so p mints and sells, gaining $\pi - 1$ per coin, likewise while the price stands. Only $\pi = 1$ admits neither trade.

The sovereign can always issue a fiat coin, so it is in M_f^0 , and a chain of mutual liquidity to it carries par along the chain with no fiat coin paid but the sovereign's.

Corollary 4.6 (Par by the Sovereign). *Let p be sovereign-connected in f , and let each of p and the persons on a simple path from p to f_σ in the f -coin holding graph fulfil every presentation of their f -denominated coins by an f -denominated coin of the next person on the path, or by a fiat coin. Then one unit of f is the only arbitrage-free price of an f -denominated p -coin, and only the sovereign pays a fiat coin.*

Proof. $f_\sigma \in M_f^0$, and a person on the path who fulfils every presentation by a coin of the next person is in M_f^{k+1} when the next is in M_f^k ; by induction from the sovereign backwards along the path, $p \in M_f$, and Proposition 4.5 applies. Every presentation but the last is fulfilled by a coin, and the last by the sovereign's fiat coin.

So, while redemptions are met, the currencies of the persons and of the sovereign are one currency, with the fiat currency as its unit of account. The coins of a person who leaves presentations unfulfilled are still debts of f , and they trade on that person's credit, as a failing bank's deposits do. Pegging each of two denominations at par imposes no constraint on the exchange rate between the two fiat currencies: by Corollary 2.4 instruments of two denominations never meet in a transaction, so no arbitrage links the two pegs, and each sovereign pegs its own denomination independently (Appendix D).

The hierarchy of money. A denomination whose sovereign has issued its grassroots coins reproduces the hierarchy of money in grassroots form: the sovereign grassroots coins are the base money of the denomination, redeemable for the fiat currency; the coins of sovereign-connected persons are inside money, in the relation commercial bank deposits bear to cash [72], without banks. A commercial

bank pegs its deposits to cash by its obligation to redeem at par on demand, backed by reserves; a grassroots issuer bears the same obligation for their coins, fulfilled in kind or by a fiat coin, and, when sovereign-connected, realised mechanically in base money. Par follows from denomination and access to the sovereign's base money while redemption obligations are met, with no separate stabilisation mechanism.

4.4 Liquidity, Solvency and Runs

The measures are per person and the results per community; both are established for grassroots currencies and bonds in [79,81], and here every coin and bond is f -denominated, the graph is the f -holding graph, and the sink is the sovereign f_σ (Definition 4.2).

The ratios. The cash, quick and current liquidity ratios of corporate finance apply to grassroots coins and bonds, with maturity in the role of asset class, and the creditworthiness measures of international monetary economics — foreign debt, current account and velocity — apply to grassroots currencies [79,81]. Under denomination they are stated in units of f , at face value, comparable across persons and with conventional balance sheets, and for a sovereign-connected issuer who meets redemptions the face value is the price (Corollary 4.6). Ratios are computed per denomination: coins and bonds of distinct denominations never meet in a transaction (Corollary 2.4), so one ratio over several denominations would count assets that cannot meet the liabilities in its denominator. The ratios separate insolvency, which no loan remedies, from illiquidity, which a loan does [81].

Solvency. A *computation* is a sequence of configurations, each reached from the previous by a transaction of Definition 2.2; it is *safe* if every step is one. The results are stated against the sink, the member with whom a community's net position is left. A set of persons containing f_σ is *sink-closed* if every edge of the f -holding graph between two vertices other than f_σ has both endpoints in the set or neither: a community whose only claims across its boundary, in f , are with the sovereign. A redemption in which the debtor is not f_σ and the instrument taken is not the debtor's own is a *clearing redemption*, and a bond returns to its issuer only as a coin, by Mature and then by a clearing redemption. The holdings of a sink-closed set V *clear* if some finite safe computation of clearing redemptions, Mature transactions and advance-date transitions of members of V leads to a configuration in which every f -denominated coin and bond of an issuer in V other than f_σ is held by its issuer [79,81].

Proposition 4.7 (Graph Solvency [79,81]). *The holdings of a sink-closed set V clear if and only if $a_p \geq \ell_p$ for every member p of V other than f_σ , and in cleared holdings each such member holds exactly $a_p - \ell_p$ sovereign grassroots coins and bonds.*

Clearing is by redemptions, in any order and with no coordination: when the condition holds, every computation in which the dates of the members advance

beyond any bound and a member who can redeem or take a matured bond for a coin eventually does reaches cleared holdings, after at most $\sum_{p \in V \setminus \{f_\sigma\}} \ell_p$ redemptions and as many Mature transactions [79,81]. The propositions quantify over safe computations and do not assume a holder can inspect the debtor's holdings; in practice a debtor incapable of set-off discloses their holdings to the redeemer.

Liquidity. For clearing, any coin or bond of the debtor may be taken; here a group needs sovereign grassroots coins, now, with no date advancing. Given a set A of persons not containing f_σ , the *liquidity of A* is the maximum, over finite safe computations of redemptions of members of A , of the number of sovereign grassroots coins members of A hold in the last configuration [79].

Proposition 4.8 (Graph Liquidity [79,81]). *The liquidity of A is the maximum flow from A to f_σ in the f -coin holding graph.*

The edges are coins already outstanding, not capacities to borrow or to route, and a member realises a path by exercising their own redemption rights one after another, with no intermediary asked to consent; a redemption that takes a bond obtains no coin and consumes the coin surrendered, so the flow is over the coins [81], and not over the matured bonds a holder could first take for coins: whether a bond is mature is subject to its issuer advancing its date, and the liquidity of a group does not depend on that. For a single person the maximum flow is the number of sovereign grassroots coins they can reach by themselves, and Proposition 4.3 is the case of one coin.

Runs on the bank. A *run on p* is a maximal finite safe computation of redemptions, each surrendering an f -denominated p -coin to p and taking a coin of an issuer other than p , within a day in which no bond is taken for a coin; it is *met in full* if no f -denominated p -coin is in circulation in its last configuration [79,81]. Let $\hat{a}_p$ and $\hat{\ell}_p$ be the out-degree and in-degree of p in the f -coin holding graph: the coins p holds and the coins p owes, their bonds being neither an asset nor a liability in the run.

Proposition 4.9 (Run on the Bank [79,81]). *Every run on p is met in full if $\hat{a}_p \geq \hat{\ell}_p$, and otherwise ends with exactly $\hat{\ell}_p - \hat{a}_p$ f -denominated p -coins in circulation, their presentations unfulfilled.*

A shortfall stands as unfulfilled presentations, evidencing the issuer's default in f . A bearer who instead takes a bond the issuer holds is met by it, as obligation 2 allows, and the run is shorter by that presentation. A run therefore stops at the issuer's holdings, and reaches the central bank only through the sovereign grassroots coins the issuer holds.

4.5 Among the Contenders

Tables 3A and 3B compare the four retail architectures [8,10], the private alternatives, and the two kinds of coin of the proposed architecture, on the structure

of a payment and on credit, cost, throughput, runs, disintermediation, the legal instrument and recovery. Bonds take no part in a retail payment and are out of both.

Every design compared but the last two places one record and one party inside every retail payment: the central bank, an intermediary, an issuer or a chain. Here every person is an issuer and keeps their own record, so the party inside a payment is the issuer of the coins paid — the central bank for a payment in sovereign grassroots coins, as in a direct central bank digital currency, and a community bank, a merchant or a neighbour for a payment in theirs. The central bank is thereby out of retail operations without an intermediary tier, and credit creation, which every other design leaves to the banks outside it, is a transaction of the currency.

Designs that preserve privacy make payments unlinkable to the operator and regulate them without revealing them: Platypus [90] combines the transaction processing of electronic cash with an account-based fund model, and PEReDi [63] distributes the record among authorities holding shares of it. Here the issuer of the coins paid is the one party to the payment beside the payer and the payee, and what the central bank sees is the circulation of its own coins.

	A. Direct	B. Hybrid	C. Intermediated	D. Indirect	E. Private DC	F. Sovereign grassroots coins	G. Non-sovereign grassroots coins
1. Retail holder's debtor	the central bank	the central bank	the central bank	an intermediary, backed by central bank money	the issuer, holding reserves (stablecoin); a bank (tokenised deposit)	the central bank	the person who issued the coins held, natural or legal
2. Retail record kept by	the central bank	intermediaries, with a copy at the central bank; the digital euro's ledger is the Eurosystem's own, centralised across three regions [46], and the digital pound's is the central bank's [18]	intermediaries; the central bank keeps a wholesale ledger	the intermediary	the issuer's ledger or a blockchain; the banks	each holder, their own holdings; the central bank the record of its coins	each holder, their own holdings; the issuer the record of their coins
3. Retail payment processed by	the central bank	an intermediary; the digital euro and the digital pound settle at the central bank [18,45]	an intermediary	the intermediary	the ledger's validators; the banks	the central bank	the issuer of the coins paid
4. Participants in a payment	payer, payee, the central bank	payer, payee, their intermediaries	payer, payee, their intermediaries	payer, payee, their intermediaries	payer, payee, the ledger or the banks	payer, payee, the central bank and the machines holding its log	payer, payee, the issuer and the machines holding their log: a person's state custodians [44], an institution's own
5. Offline payment	by value stored on the device, at the holder's or the operator's risk	the same	the same	the same	no	no: the central bank and the machines holding its log must be reachable	not offline from the issuer; over Bluetooth or a local network that reaches the issuer and the machines holding their log, including one with no connection to the Internet
6. Who sees a payment	the central bank	the intermediary and the central bank	the intermediary; the central bank in aggregate	the intermediary	the ledger's operator, or everyone on a public chain; the banks	payer, payee and the central bank	the three parties; the machines holding the issuer's log record it, and their persons cannot read it [44]
7. Retail balances by identity at the central bank	not necessarily; the central bank keeps the retail record	no	no	no	no	no: the central bank keeps the record of its own coins	no

Table 3A. CBDC architectures [8,10]: part A, the structure of a payment. Columns F and G are the two kinds of coin of the proposed architecture, the central bank's and every other person's; a grassroots currency comprises the coins and the bonds of its issuer, and bonds take no part in a retail payment. Of the CBDCs compared, the e-CNY [88], the Sand Dollar [33], the eNaira [32] and JAM-DEX [19] are hybrid [24], and so is Chaumian eCash [25,34], with an anonymous payer; the digital euro [45] and the digital pound [18] are two-tier, distributed by private intermediaries with the ledger kept and payments settled at the central bank; Project Hamilton [69] is a system design for a direct core; the intermediated [9] and the indirect [4,8] architectures are proposals; the private alternatives are regulated stablecoins [1,2,56] and tokenised deposits [50]. Rows 5 and 6 are properties of the implementations cited and not of the architecture class, offline support and who sees a payment being design choices within each.

	A. Direct	B. Hybrid	C. Intermediated	D. Indirect	E. Private DC	F. Sovereign grassroots coins	G. Non-sovereign grassroots coins
8. Credit creation within the architecture by	no one: a central bank liability	no one	no one	no one: fully backed	no one (stablecoin); the banks (tokenised deposit)	the central bank, by its mutual credit lines	every person, by issuing their own coins
9. Cost of a payment	the central bank's processing	the intermediary's, fees by policy	the same	the same	the chain's fees; the banks' fees	operating a device; no fee required by the architecture	operating a device; no fee required by the architecture
10. Throughput bounded by	the central bank's processor	the central bank's ledger and the intermediaries	the intermediaries	the intermediaries	the chain; the banks' systems	the central bank and the machines holding its log	no component shared by all issuers; grows with the issuers and their custodians
11. Where a run goes	from bank deposits into the CBDC, at the speed of conversion	the same	the same	into the intermediary's backing	onto the issuer's reserves; onto the bank	onto one issuer, met from their holdings; what the public can obtain of central bank money is bounded by what the central bank has issued and not taken back	
12. Disintermediation mitigant	holding limits, tiered remuneration, waterfall	the same	the same	none needed: the claim is on the intermediary	a tokenised deposit needs none, the claim staying on the bank [50]; for a stablecoin none is proposed, the mitigants proposed addressing runs—issuance through banks, or full backing with safe assets [56]	none needed to bound demand-driven creation: no holder of a bank deposit has a right to newly issued sovereign grassroots coins, which enter in exchange for fiat coins, by the central bank's payments and by its mutual credit lines, all at its own election	
13. Legal instrument	a new central bank liability, by legislation	the same	the same	e-money or deposit law	stablecoin regulation; deposit law	a signed debt of the central bank, analogous to a promissory note; the authority to issue it is statutory [17]	a signed debt of its issuer, analogous to a promissory note, under the ordinary rules of contract
14. Recovery of a lost key or device	by identity, from the central bank's record, where access is as the token design provides, where token-based [8,24]	by identity, from the intermediary's record or the central bank's copy, where account-based (the eNaira, the e-CNY); as the token design provides, where token-based (the Sand Dollar, JAM-DEX) [24]	by identity, from the intermediary's record, where account-based; as the token design provides, where token-based	the same	a bearer instrument [50], held by whoever holds the key; a tokenised deposit from the bank's record	from the central bank's log, their identity from their custody [44]; an institution's log from its own machines	holders from the issuers' logs; a person's own log, exactly, and their identity from their state and identity custodians [44]; an institution's log from its own machines

Table 3B. CBDC architectures, part B: credit, cost, throughput, runs, disintermediation, the legal instrument, and recovery from the loss of a key or device; the columns are those of part A. Rows 11 and 12 hold of the two kinds of coin together and are not properties of either. Rows 9 and 14 are properties of the implementations cited and not of the architecture class, the cost of a payment and the recovery of a lost key being design choices within each.

5 Interest: Grassroots Bonds

With grassroots bonds, credit acquires time and a price. Here we add bonds to the coins of Sections 2 and 4, present the instruments formed from coins and bonds, and the central bank's instruments of monetary policy as transactions in its coins and bonds.

5.1 Maturity and Interest

A coin and a bond are distinct instruments (Section 2.1): a coin is a unit of its issuer's debt due now and carries no date, and a bond is that unit due at its date. A coin may be paid, and presented to its issuer for redemption. A bond may be minted, swapped, escrowed and sold, and an issuer may fulfil a presentation with one; it is neither paid nor presented, and once it is mature its bearer may take a coin of its issuer for it [81].

Coins are demand instruments and bear no interest. Interest is borne by bonds, as the difference between the face value of a bond and the coins swapped for it: a lender who advances k coins against bonds of face value $k(1+\rho)$ maturing at d lends at the rate ρ for that maturity; ρ is the return over the term, not an annual rate, and rates of unlike terms are compared after annualisation. A swap of coins for coins is at par and on demand, so it carries no interest — prompt redemption after it would return any premium (Section 4.2) [81] — and the discount at which coins are swapped for a bond, with its maturity, is the rate.

Maturity is judged by the date of the issuer, which the issuer warrants when a matured bond of theirs is taken for one of their coins; an issuer whose date lags behind the calendar breaches that warranty, and the record of the transaction witnesses the breach against them [81]. The obligation of a coin is enforced by the contract; that of a bond as a whole is attested, and enforceable at law on the record (Appendix A).

5.2 The Instruments

Every person can lend at interest, sell debt, open term credit lines, post collateral, issue deposit-like claims, and form the further financial instruments; each is a swap of bonds or an escrow agreement [81]. A zero-coupon loan is a swap of freshly minted coins for the borrower's bonds of larger face value maturing later; a sale of debt before maturity is a swap of a third person's bonds for coins at a discount; a forward is a swap of bonds of the two parties maturing at one date. With an escrow agent, trusted by the parties for that agreement and holding the bonds it transfers by the agreed conditions, come loans with payment schedules, term credit lines with draws, options, collateral, guarantees, insurance, credit default swaps and letters of credit. Every instrument is stated in Appendix B, recalled from [81].

A term credit line is the escrow instrument the central bank uses, and differs from the mutual credit line of Section 4.2, which is a swap of coins at par and on demand: the lender deposits its coins with the escrow agent up to the agreed

limit, the borrower draws by depositing principal and coupon bonds, the agent releases the two sides crosswise, and at expiry the undrawn balance returns to the lender [81]. A draw is therefore a transaction the lender has consented to in advance and the borrower elects, and each tranche falls due at its own maturity.

A bank's coins play the economic role of its demand deposits (Section 4.1) and its bonds that of its term deposits, and it lends by swapping its coins for its borrowers' bonds, at rates it sets. A saver who holds a bank's bond holds a dated claim on the bank, and sells it before maturity at a discount rather than breaking a deposit.

5.3 The Central Bank's Instruments

The central bank's instruments of monetary policy are the same transactions, and it chooses the counterparty, amount, rate, maturity and collateral of its credit operations; the counterparty of an open market operation is whoever holds the security. Lending to a named city, firm or household is credit policy as much as monetary policy, and which it is, and whether the central bank may do it at all, is a matter of its mandate, which we take as given.

Goodfriend [54] draws the distinction: an open market operation in government securities returns its revenue to the fiscal authorities, while lending to particular borrowers allocates public funds and is debt-financed fiscal policy. He would therefore confine a central bank to last-resort lending to solvent supervised institutions, unless the fiscal authorities agree in advance. Cúrdia and Woodford [38] treat such lending as a dimension of policy distinct from the interest rate, worth using when private intermediation is impaired but costly in itself; the case for it depends on the market lent into, and the size of a spread does not settle it. The central bank can make such loans under this architecture; whether it should do so is a question of its mandate.

The policy rate. The policy rate is the rate at which the central bank lends its coins against bonds: it advances k of its coins against a counterparty's bonds of face value $k(1 + \rho)$ maturing at d , and ρ , the return over that term, is the rate. A change of policy changes the terms of new swaps, and no bond already issued.

Targeted liquidity. A mutual credit line is targeted liquidity without a rate (Section 4.2); with maturity it acquires one. Targeted liquidity at a rate is a term credit line to a city, a bank, a firm or a community, whose tranches are drawn the central bank has consented to, each falling due at its maturity. A city struck by a disaster draws the central bank's coins against its own city bonds and funds relief in coins redeemable at face value in sovereign money. As the city repays, it acquires sovereign grassroots coins and redeems them from the central bank against its principal bonds, which the central bank cannot refuse, and the undrawn balance returns to the central bank at expiry; a tranche already drawn falls due at its own maturity, and the central bank does not recall it. The recipient, the amount, the maturity and the rate are the parameters of the transactions, and who drew, who repaid and what remains outstanding is their record. Where conventional policy transmits unevenly across time and

sectors, and weakly in recessions [74,82], here the central bank contracts with the intended recipient and no intermediation stands between.

Lender of last resort. A run exhausts the coins an issuer holds, and their remaining bonds may cover their liabilities while their coins do not: the failure is of liquidity and not of solvency, and the ratios distinguish the two (Section 4.4). In a panic no one lends even against good bonds, so the central bank does: it opens an emergency term credit line with the distressed issuer, advancing its coins against their bonds, collateralised by their remaining holdings, at a penalty rate above the policy rate. This is Bagehot’s prescription [12], to lend freely against good collateral at a penalty rate, as a swap of bonds; it differs from the lending above in the counterparty’s condition, the collateral and the rate.

The central bank’s own bonds. With its own bonds — interest-bearing liabilities it issues to the counterparties it chooses — the central bank absorbs liquidity from those counterparties, on terms set at issuance, with no tier and no cap imposed by the architecture. A counterparty swaps the central bank’s coins now for its bonds maturing later, and holds the safest dated claim in the denomination.

Open market operations. The central bank buys and sells government and bank bonds for its coins, which are its open market operations; a purchase puts its coins into circulation against a bond it then holds, and a sale takes them back. Securities that are not grassroots bonds are bought and sold for its coins in the same way, by a payment against delivery outside the currency.

Where interest is borne. Interest is charged on the borrowing of sovereign grassroots coins and paid on the bonds the central bank issues to the counterparties it chooses. The coins themselves bear none, as cash does not, so they introduce no interest-rate competition with deposits; a claim that bears no interest can still be preferred for its safety or its convenience — India’s digital rupee, which bears none and is capped, reduced the retail deposits of the banks exposed to it by 2.7%, concentrated in liquid savings accounts [41] — and the central bank’s issuance bounds the coins in circulation (Section 4.2). A remunerated central bank digital currency pays its rate to whoever holds it and so competes with deposits, which is one reason neither the digital euro nor the digital pound is to be remunerated [18,46]; the Eurosystem states that holdings would not be remunerated and would be subject to holding limits, to preserve the role of banks in providing credit [46].

What the other proposals leave outside. The retail proposals compared add a retail form of central bank money and leave the central bank’s lending, its asset purchases and the implementation of the policy rate in reserves, an instrument the public does not hold. Here they are transactions in the coins and bonds the public holds.

5.4 A Counterparty-Specific Rate Corridor

The central bank sets two rates for a counterparty: the rate at which it lends its coins against that counterparty's bonds, and the rate it pays on its own bonds issued to them. We argue that the two bound the rates the counterparty faces, at like maturity, collateral and risk. The corridor is counterparty-specific. We argue a bound on the rates one admitted counterparty faces; we do not argue the overnight interbank corridor of today's operational frameworks [3], nor the transmission of policy to output and prices. The argument assumes that a person takes the cheaper of two credits available to them on like terms, and the dearer of two claims.

The upper bound. A counterparty who can still borrow from the central bank does not pay more than its lending rate. A lender who asks more offers, at like maturity, collateral and risk, a credit the counterparty already has on better terms, and the counterparty draws on the central bank instead. So the rate the counterparty pays is at most the central bank's lending rate.

The lower bound. A counterparty who can still acquire the central bank's bonds does not accept less than the rate on them. A borrower who offers less offers, at like maturity, a dated claim no safer than the central bank's — whose issuer can always issue a fiat coin (Section 2.2) — at a lower rate, and the counterparty buys the central bank's bond instead. So the rate the counterparty accepts is at least the rate on the central bank's own bonds.

Whom the corridor binds. Both bounds hold while the counterparty can act on them: the term credit line is not exhausted and its collateral suffices, and the central bank is still issuing its bonds to them. Both conditions are quantities the central bank sets, so it admits to the corridor the counterparties it chooses, and a counterparty it does not admit borrows and lends on their own credit. Today the standing facilities [3] bound the rate at which banks lend to one another, one corridor for the interbank tier; here the corridor is counterparty-specific and the counterparties are whoever the central bank admits — a bank, a city, a firm, a cooperative, a household — and the instruments are the coins and bonds the public holds, so the corridor binds at the tier the central bank chooses, not solely at the interbank tier.

5.5 Among the Types of Money

Table 4 sets the three components beside the types of money proposed as a retail central bank digital currency or in its place — account-based and token-based designs, regulated stablecoins, and tokenised deposits — by whose liability each is, what backs it, where its record is kept, how it is created, whether it bears interest, and what can be done with it. Cash, deposits, cryptocurrencies and community currencies are not proposed as a central bank digital currency and are out of it. A grassroots bond is a dated claim and is not paid; its bearer takes a coin of its issuer for it once it is mature, so its column is credit and not money.

	A. Account-based	B. Token-based	C. Regulated stablecoins	D. Tokenised deposits	E. Sovereign grassroots coins	F. Non-sovereign grassroots coins	G. Grassroots bonds
1. Whose liability	the central bank's [14]	the central bank's [14]	the issuer's [56]	the bank's [50]	the central bank's [79]	each person's, natural or legal [79]	its issuer's, the central bank or any other person [81]
2. Backing and redemption	central bank money itself; convertible at par with cash [14]	central bank money itself; convertible at par with cash [14]	reserves of cash and short-term government debt; redeemable at par [1,2], though not always accepted at par in the market [56]	as deposits; transfers settled in central bank money [50]	the fiat currency the central bank issues; redeemed at par into fiat coins on presentation	the issuer's goods and services and the coins they hold; redeemed at par against any coin they hold, and along chains of liquidity into sovereign grassroots coins [79]	as its issuer's coins: once the date of its maturity, its bearer may take a coin of the issuer for it [81]
3. Record	balances by identity, on the central bank's ledger or intermediaries' [8, 24]; the eNaira, the digital euro and the digital pound [17,24,46]	tokens held by key [8,24]: blind-signed coins with a spent list at the central bank [25,34], an unspent-output set [69]; the Sand Dollar and JAM-DEX [24] in the implementations compared, issued by the central bank against bank money converted into it [24]	a blockchain; a bearer instrument [50]	the bank's ledger, or a unified ledger [50]	the central bank's log, on its own machines	each person's log of their own coins, backed up by their custodians [44,79]; an institution's log on its own machines	the log of its issuer, as its coins
4. Creation and entry into circulation	implementations compared, issued by the central bank against bank money converted into it [24]	in the implementations compared, issued by the central bank against bank money converted into it [24]	issued against fiat received	created by the bank's lending, as deposits [72]	minted by the central bank, entering in exchange for fiat coins, by its payments, and by its mutual credit lines against the counterparty's coins or, with bonds, their bonds	minted by each person, entering by mutual credit, coins for coins	minted by its issuer, entering by loans, coins for bonds
5. Interest	a design choice; the implementations compared bear none [18,88]	a design choice; the implementations compared bear none [19,34]	the token bears none	as deposits	none, as on cash	none	the discount at which coins are swapped for them [81]
6. Operations	payment and conversion, under holding limits, tiers and waterfalls [15]	payment and conversion	payment on the chain; redemption by the issuer's direct customers [56]	payment and transfer; the bank's lending beside it	payment and redemption; the central bank's mutual credit lines	payment, mutual credit and redemption	credit: for the central bank the policy rate, targeted liquidity, the lender of last resort, its own bonds and open market operations; for every other person loans at interest, sale of debt, term credit lines, collateral and the escrow instruments [81]

Table 4. Types of money proposed as a retail central bank digital currency or in its place, and the credit instrument beside them: whose liability each is, what backs it and how it is redeemed, where its record is kept, how it is created and enters circulation, whether it bears interest, and what can be done with it; all have the fiat currency as their unit of account. Columns A and B are the designs of Tables 3A and 3B by the form of the money. Columns E, F and G are the three components of the proposed architecture; a grassroots bond is a dated claim: it is not paid, and its bearer takes a coin of its issuer for it once the date of its issuer has reached its maturity, so column G is credit and not money.

6 Related Work

Central bank digital currency. The requirements of a retail central bank digital currency [14], its financial-stability implications [15] and its system design [16] are the reports this paper is checked against in Section 3; the four architectures [8,10], the currencies in operation and in preparation, the system designs, and the private alternatives are compared with the proposal in Section 4.5 and in Tables 3A and 3B, and surveyed in [78]. Kumhof and Noone [65] are the precedent for issuance that is not by conversion: their four principles include no guaranteed on-demand convertibility of bank deposits into the currency, and issuance only against eligible securities. Their central bank buys securities its counterparty already holds; here it lends against coins its counterparty issues, and the counterparty is whoever it chooses (Section 4.2).

The currency as an instrument of monetary policy. A central bank digital currency that bears interest has been proposed as an instrument of policy. Bordo and Levin [26] would make it account-based and interest-bearing, make its rate the main tool of policy, and remove the effective lower bound by a graduated schedule of fees on transfers between cash and the currency. Davoodalhosseini [40] studies optimal monetary policy where agents hold cash, such a currency, or both, and finds that where the cost of using it is not too high it implements more efficient allocations than cash and can attain the first best, and the central bank can make what it pays contingent on the balance held; Agur, Ari and Dell’Ariccia [5] derive the optimal design where agents sort into cash, the currency and deposits by their preferences over anonymity and security, and find that a deposit-like currency depresses bank credit and output while a cash-like one may drive cash out, and an interest-bearing currency eases the tradeoff where network effects matter. The second limitation of Section 1 is therefore of the designs in operation and in preparation, in which the currency is a payment liability and policy operates through reserves, and not of the concept. The coins here bear no interest. The architecture adds the central bank’s lending, its bond issuance and its open market operations, as transactions in the coins and bonds the public holds (Section 5.3).

Deposits, recycling and disintermediation. Whether the substitution of public for private money matters depends on what the central bank does with the funding that reaches it. Brunnermeier and Niepelt [28] give conditions under which a swap of private for public money leaves the allocation and the price system unchanged, when the central bank passes the funds back to the banks that lost them, so that a central bank digital currency need imply neither a credit crunch nor a loss of financial stability; Kim and Kwon [64] show that where the deposits taken are not lent back, credit supply falls, and that lending them back to the banks raises both credit supply and stability; Fernández-Villaverde, Sanches, Schilling and Uhlig [48] have the central bank intermediate through investment banks: its contract with them is not callable, so it cannot be run on, and it becomes the deposit monopolist, which may endanger maturity transformation; and the review of Infante, Kim, Orlik, Silva and Tetlow [59] finds that

the effect on banks depends on how the central bank recycles the new liability, by asset purchases or by lending. Keister and Sanches [62] set the efficiency of exchange against the crowding out of deposits, and show that a currency targeted to compete only with cash or only with deposits can raise welfare where a single universal one need not; Chiu, Davoodalhosseini, Jiang and Zhu [35] show that where banks have market power in the deposit market a currency remunerated in an intermediate range raises the deposit rate and with it bank lending and output, and its rate acts as a floor under the deposit rate. Bidder, Jackson and Rottner [22] separate the two horizons: slow disintermediation, which shrinks a fragile banking system in normal times and stabilises it, and fast disintermediation in a run, which a currency invites because, unlike cash, it can be held at scale at no cost, so a holding limit keeps the first without the second. The one live retail currency studied bears this out at the slow horizon: Di Maggio, Ghosh, Ghosh, Vats and Wu [41] find that eligibility for India's digital rupee, which bears no interest and is capped, lowered retail deposits by 2.7%, concentrated in liquid savings accounts and not in term deposits, that credit fell and then recovered as banks changed their funding mix, and that the currency displaced deposit-backed digital payments rather than cash. Each of these concerns a currency the public obtains by converting deposits into it. Here there is no such flow to recycle: no holder of a deposit has a right to newly issued sovereign coins, the central bank issues them to the counterparties it elects against coins those counterparties issue (Section 4.2), and the credit a bank loses is created by the persons themselves. The coins bear no interest, so they introduce no interest-rate competition with deposits; a claim that bears none may still be preferred for its safety or its convenience, and the central bank's issuance bounds the quantity in circulation.

The operational framework of policy. Abad, Nuño and Thomas [3] analyse what a central bank digital currency does to the framework in which policy is implemented: its adoption contracts deposits, and the contraction is absorbed first by a fall in excess reserves and, if it is large enough, by recourse to central bank credit; the system moves from a floor to a corridor and then to a ceiling, and the effect on credit, investment and output differs with the framework it reaches. The corridor of Section 5.4 is of another kind. It is counterparty-specific, and bounds the rates one admitted counterparty faces at like maturity, collateral and risk; theirs is the corridor between the standing facilities, which bounds the rate at which banks lend to one another. Lending to a named city, firm or household is credit policy as much as monetary policy, and whether a central bank may allocate credit in that way is a question of its mandate, which this paper takes as given (Section 5.3).

Synthetic central bank digital currency. A synthetic central bank digital currency [4] has private firms issue digital liabilities backed one for one by central bank reserves, so that private provision rests on a public anchor. Denominated grassroots coins take the opposite choice. Their issuers create credit, bear their own default, and hold no reserve against their coins, and their holders reach base money by redemption along chains of liquidity (Proposition 4.3) rather than by

backing. The two put different things behind a privately issued claim of a fiat unit: reserves held against it, or an obligation realised by redemption.

What the mitigants bound. The measures proposed against deposit flight — limits on holdings and on transactions, tiered remuneration and waterfalls [15,46], Bindseil’s two-tier remuneration, which he offers as the simpler alternative to Kumhof and Noone’s principles, where the first tier stays attractive and never negative and the second is priced to discourage the currency as a store of value [23], and Kumhof and Noone’s own refusal of guaranteed convertibility between the currency and reserves and between deposits and the currency [65] — bound a demand that the design admits. The Bank of England has measured the effect of such a limit: under its severe illustrative stress, with no individual limit some 21% of the banks modelled fall below a 100% liquidity coverage ratio and the demand for central bank lending reaches about £252 billion, against 9 to 12% and £21 to £112 billion at individual limits of £5,000 to £20,000, and the limit is traded off against what households can do with the money [37]. Here there is no such demand to bound: the outstanding coins and bonds are those the central bank has issued and has not taken back (Lemma 2.3), so the quantity is settled at issuance and maturity only changes its composition; a limit for other reasons is left to the deployment. Each ingredient has a literature: the currency as an instrument of policy, interest-bearing central bank liabilities, disintermediation mitigated by design, central bank lending in place of displaced deposit funding, a hierarchy of public and private digital money, a rate corridor, and privately issued fiat-denominated digital liabilities anchored to central bank money. Here we proposed their conjunction (Section 7).

Grassroots currencies and bonds. Grassroots coins and bonds [79,81] are units of debt issued by any person, with mutual credit formed by their exchange, redemption pegging mutually-liquid currencies to each other, financial instruments as swaps of bonds and escrow agreements, and the solvency, liquidity and run results this paper specialises. They are undenominated, with no external unit of account. This paper adds denomination, which makes every coin a debt of a fiat currency, the sovereign, and par by arbitrage.

Stablecoins. Fiat-backed stablecoins peg a token to a fiat currency by the issuer’s obligation to redeem at par, backed by reserves of cash and short-term government debt [56]; redemption is off-chain and typically restricted to direct customers, other holders realising the peg by selling at the market rate. Regulation now mandates the obligation: the GENIUS Act in the United States [2] and MiCA in the European Union [1] require at-par redemption rights and full reserve backing. The obligation of Definition 2.1 parallels that statutory right, borne by every issuer rather than by one. A stablecoin has one issuer, whose pooled reserves back all tokens, and its holder’s claim is on those reserves; here every person issues their own currency and bears the obligation for it, and the holder’s claim is on the issuer, in fiat, fulfilled in kind and, through chains of liquidity, in the sovereign’s base money (Proposition 4.3).

Commercial bank money and free banking. Commercial bank deposits are privately issued money pegged at par to fiat by the bank’s obligation to redeem

in cash on demand [72], and in modern systems by settlement in central bank money, prudential regulation, deposit insurance and the lender of last resort beside it [12,50]; the note-issuing banks of the free-banking episodes had the obligation and no such backstops behind their notes [77,87]. A denomination whose sovereign has issued its grassroots coins reproduces the deposit-to-cash peg without banks: the sovereign's coins take the place of cash, a sovereign-connected person's coins the place of deposits, and the redemption chain the place of the teller (Section 4.3). Grassroots coins are inside money [30,31]; the sovereign's coins are the outside money grassroots currencies lacked; and in the framework of digital currency competition [27] such a denomination is a currency area whose unit of account is the fiat unit, joined by holding, issuing or accepting its coins rather than by treaty [6,73].

Bills of exchange and promissory notes. Before banks dominated payment, debts circulated as bills of exchange and promissory notes — signed promises to pay a fixed sum of a currency at a set date — traded and discounted before maturity [75,76]; a grassroots bond is such an instrument in digital form [81]. Denomination fixes the sum promised in a unit of a fiat currency, which those instruments had and grassroots bonds lacked (Definition 2.1).

Financial networks. Eisenberg and Noe [42] model an economy of interbank obligations and prove that a clearing payment vector exists as a fixed point, grounding the analysis of contagion and systemic risk [52]; Karlan, Mobius, Rosenblat and Szeidl [61] define network-based trust as a maximum flow of social collateral over trust links, and in credit networks a payment goes through exactly when the maximum credit flow from payer to payee covers it [39]. How grassroots clearing differs — unit bonds redeemed in kind at the holder's initiative rather than paid pro rata in a common numéraire, a comparison of counts person by person, and a maximum flow over bonds already outstanding rather than over capacities to borrow or to route — is set out in [79]. Under denomination the counts and the flow are in the fiat unit and the designated member is the sovereign, so what a group can realise now is base money (Section 4.4).

Monetary transmission. Olivei and Tenreiro [74] show that the output effect of a monetary policy shock depends on its timing within the year, as staggered wage-setting absorbs shocks arriving just before contracts reset, and Tenreiro and Thwaites [82] that the effects on output and inflation are much smaller in recessions. Both concern one economy-wide instrument whose incidence is set by the economy's structure. Here the incidence is a contract: a term credit line names its counterparty, amount, rate and timing, and the lender of last resort lends to the distressed issuer directly (Section 5.3), while the policy rate remains, as the rate at which the central bank lends its coins against bonds. The architecture thereby bypasses intermediary allocation for the named recipient; the aggregate effect on output and prices is a separate question, which this paper does not settle.

Community and complementary currencies. Mutual credit systems such as Sardex [60] and community currencies such as Sarafu [71] create liquidity from trust within a community, and their units are typically pegged by convention to

the national currency, a peg maintained by the operator’s policy rather than by redemption. Personal-currency systems [36,49,58] and credit networks [39] carry liquidity over trust edges as grassroots currencies do. A denomination whose sovereign has issued its grassroots coins gives such systems what convention cannot: redemption at face value, terminating at the sovereign issuer of the unit they already price in.

Hawala. Hawala transfers value across borders without moving money: a customer pays a broker locally, a counterpart broker pays the recipient in their own locale, and the brokers along the path carry the resulting obligations on open mutual account, settled later by reverse transfers, trade or netting, at rates they quote; trust and reputation within the brokers’ network take the place of contracts and collateral [70]. Grassroots currencies realise the mechanism: brokers are persons with mutual credit, a transfer is a chain payment across mutually-liquid currencies, and settlement among brokers is set-off. Denomination adds what hawala lacks: the obligations are legally binding debts of the fiat units and are recorded, where hawala’s informality and opacity ground the regulatory concern, and exchange across denominations needs no broker pair, as persons exchange directly, by escrow, both legs completing or neither (Appendix D).

Community credit institutions. Community credit sustains lending among neighbours without courts or physical collateral: credit cooperatives rely on peer monitoring and local sanctions [13,57], group lending on joint liability — *social collateral*, repayment secured by the borrower’s standing with their community [20,51] — and rotating savings and credit associations on community-based mutual commitment [21]. Caselli and Gennaioli [29] model the failure of meritocracy brought about by imperfect contract enforcement, which prevents the transfer of control over productive assets from the untalented rich to the talented poor; credit secured by social collateral and enforced by the protocol reaches borrowers that courts and asset-based lending do not. How grassroots credit differs, the sanction carried by the record and the liability individual, each person issuing their own currency and bearing their own default, is set out in [81]. Under denomination such an institution’s currency has the fiat unit its books are already kept in, and a claim on it is a debt of that unit (Definition 2.1).

7 Conclusions

A central bank digital currency built of grassroots currencies has three components and one contract: the sovereign joins the currency the persons operate as one more issuer, and does not need a separate protocol. Sovereign grassroots coins are money: digital debts of one unit of the fiat currency, issued by the central bank, held and paid by the public, a direct central bank digital currency by themselves. We check them against the three foundational principles and the fourteen core features of [14]: offline payment is not met; several of the others hold by construction or by the protocols the architecture rests on; and the throughput, resilience and ease of use of a deployment, and the central bank’s authority to issue, remain to be established (Sections 2 and 3). The non-sovereign

grassroots currencies add credit: the central bank issues its sovereign grassroots Dollar coins by mutual credit lines against Dollar-denominated grassroots coins by persons of its choice. Redemption runs the other way: redeeming a sovereign coin gives up the coin and takes a fiat coin, so the coins in circulation fall. Nothing obliges the central bank to mint a new sovereign coin against a bank deposit: a depositor who wants one buys it from a holder, or their bank pays them out of its cash or the coins it already holds. A flight from deposits therefore moves coins that already exist and creates none, so no holding limit, tier or waterfall is needed to bound the creation of central bank money (Section 4). Grassroots bonds add maturity, and with it interest, the standard financial instruments, and the central bank’s instruments of monetary policy (Section 5). With them the central bank lends, absorbs liquidity, sets its rates and buys and sells securities in the coins and bonds the public holds, choosing the counterparties and terms of its credit operations.

The peg has two legs: the issuer’s obligation, worth the issuer’s credit, and redemption along chains of mutual liquidity into the sovereign’s base money (Proposition 4.3). One unit of the fiat currency is then the only arbitrage-free price of the coins of an issuer who meets presentations (Proposition 4.5, Corollary 4.6), so while redemptions are met the currencies of the persons and of the sovereign are one currency, with the fiat currency as its unit of account. The central bank’s lending rate and the rate on its own bonds bound from above and from below the rates its counterparties face, at like maturity, collateral and risk, and it admits to that corridor the counterparties it chooses (Section 5.4).

Each ingredient has a literature (Section 6). Here we proposed their conjunction: a retail coin of the central bank, countersigned by it, in the same contract as the fiat-denominated coins of persons; credit created between two persons, with no shared ledger; redemption chains that carry the sovereign peg; and maturity and escrow, which extend the same instruments to lending and to the operations of monetary policy. The design lacks what the currencies in operation have: measured throughput, deployed scale and a measured ease of use; it rests on a prototype realisation [43,44,67]. A digital economy of non-sovereign grassroots currencies can form without the central bank of the denomination, spontaneously or by spilling over from a neighbouring economy, and the central bank can join it once formed by issuing its own denominated grassroots coins, which are then the sovereign ones.

AI Disclosure. We used Anthropic’s Claude models to assist with the prose of this paper, for drafting and proofreading: we specified the content, reviewed every passage against the sources and against the papers this one builds on, and made all design decisions. We verified the correctness and originality of all content, including all references. Responsibility for all content rests with us.

References

1. Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA). European Parliament and Council (2023)

2. Guiding and establishing national innovation for US stablecoins act (GENIUS act). Public Law 119-27, United States (2025)
3. Abad, J., Nuño, G., Thomas, C.: CBDC and the operational framework of monetary policy. *Journal of Monetary Economics* **151**, 103762 (2025). <https://doi.org/10.1016/j.jmoneco.2025.103762>
4. Adrian, T., Mancini-Griffoli, T.: The rise of digital money. IMF Fin-Tech Notes 19/01, International Monetary Fund (Jul 2019), <https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>
5. Agur, I., Ari, A., Dell'Ariccia, G.: Designing central bank digital currencies. *Journal of Monetary Economics* **125**, 62–79 (2022). <https://doi.org/10.1016/j.jmoneco.2021.05.002>
6. Alesina, A., Barro, R.J., Tenreyro, S.: Optimal currency areas. In: NBER Macroeconomics Annual 2002, vol. 17, pp. 301–345. MIT Press (2002)
7. American Law Institute and Uniform Law Commission: Uniform commercial code, article 3: Negotiable instruments (2002)
8. Auer, R., Böhme, R.: The technology of retail central bank digital currency. *BIS Quarterly Review* pp. 85–99 (Mar 2020), https://www.bis.org/publ/qtrpdf/r_qt2003j.htm
9. Auer, R., Böhme, R.: Central bank digital currency: the quest for minimally invasive technology. *BIS Working Papers* 948, Bank for International Settlements (Jun 2021), <https://www.bis.org/publ/work948.htm>
10. Auer, R., Cornelli, G., Frost, J.: Rise of the central bank digital currencies: drivers, approaches and technologies. *BIS Working Papers* 880, Bank for International Settlements (Aug 2020), <https://www.bis.org/publ/work880.htm>
11. Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice, T., Shin, H.S.: Central bank digital currencies: Motives, economic implications, and the research frontier. *Annual Review of Economics* **14**, 697–721 (2022). <https://doi.org/10.1146/annurev-economics-051420-020324>
12. Bagehot, W.: *Lombard Street: A Description of the Money Market*. Henry S. King & Co., London (1873)
13. Banerjee, A.V., Besley, T., Guinnane, T.W.: Thy neighbor's keeper: The design of a credit cooperative with theory and a test. *The Quarterly Journal of Economics* **109**(2), 491–515 (1994)
14. Bank of Canada and European Central Bank and Bank of Japan and Sveriges Riksbank and Swiss National Bank and Bank of England and Board of Governors of the Federal Reserve and Bank for International Settlements: Central bank digital currencies: Foundational principles and core features. Joint Report 1, Bank for International Settlements (2020), <https://www.bis.org/publ/othp33.htm>
15. Bank of Canada and European Central Bank and Bank of Japan and Sveriges Riksbank and Swiss National Bank and Bank of England and Board of Governors of the Federal Reserve System and Bank for International Settlements: Central bank digital currencies: financial stability implications. Report 4, Bank for International Settlements (Sep 2021), https://www.bis.org/publ/othp42_fin_stab.pdf
16. Bank of Canada and European Central Bank and Bank of Japan and Sveriges Riksbank and Swiss National Bank and Bank of England and Board of Governors of the Federal Reserve System and Bank for International Settlements: Central bank digital currencies: system design and interoperability. Report 2, Bank for International Settlements (Sep 2021), https://www.bis.org/publ/othp42_system_design.pdf

17. Bank of England: Progress update: Digital pound design phase. Tech. rep., Bank of England (Mar 2026), <https://www.bankofengland.co.uk/the-digital-pound/progress-update-digital-pound-design-phase>
18. Bank of England and HM Treasury: The digital pound: A new form of money for households and businesses? Consultation paper, Bank of England (Feb 2023), <https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper>
19. Bank of Jamaica: JAM-DEX: Jamaica's central bank digital currency. <https://boj.org.jm/core-functions/currency/cbdc/> (2022)
20. Besley, T., Coate, S.: Group lending, repayment incentives and social collateral. *Journal of Development Economics* **46**(1), 1–18 (1995)
21. Besley, T., Coate, S., Loury, G.: The economics of rotating savings and credit associations. *American Economic Review* **83**(4), 792–810 (1993)
22. Bidder, R., Jackson, T., Rottner, M.: CBDC and banks: disintermediating fast and slow. BIS Working Papers 1280, Bank for International Settlements (Jul 2025), <https://www.bis.org/publ/work1280.htm>
23. Bindseil, U.: Tiered CBDC and the financial system. ECB Working Paper Series 2351, European Central Bank (Jan 2020). <https://doi.org/10.2866/134524>
24. BIS Consultative Group on Innovation and the Digital Economy: A proposal for a retail central bank digital currency (CBDC) architecture. Cgide report, Bank for International Settlements (Dec 2024), <https://www.bis.org/publ/othp89.pdf>
25. BIS Innovation Hub: Project Tourbillon: exploring privacy, security and scalability for CBDCs. Tech. rep., Bank for International Settlements (Nov 2023), <https://www.bis.org/publ/othp80.pdf>
26. Bordo, M.D., Levin, A.T.: Central bank digital currency and the future of monetary policy. NBER Working Paper 23711, National Bureau of Economic Research (Aug 2017), <http://www.nber.org/papers/w23711>
27. Brunnermeier, M.K., James, H., Landau, J.P.: The digitalization of money. Working Paper 26300, National Bureau of Economic Research (2019). <https://doi.org/10.3386/w26300>
28. Brunnermeier, M.K., Niepelt, D.: On the equivalence of private and public money. *Journal of Monetary Economics* **106**, 27–41 (2019). <https://doi.org/10.1016/j.jmoneco.2019.07.004>
29. Caselli, F., Gennaioli, N.: Dynastic management. *Economic Inquiry* **51**(1) (2013)
30. Cavalcanti, R.d.O., Wallace, N.: Inside and outside money as alternative media of exchange. *Journal of Money, Credit and Banking* pp. 443–457 (1999)
31. Cavalcanti, R.d.O., Wallace, N.: A model of private bank-note issue. *Review of Economic Dynamics* **2**(1), 104–136 (1999)
32. Central Bank of Nigeria: Design paper for the eNaira. Tech. rep., Central Bank of Nigeria (Oct 2021), <https://www.enaira.gov.ng/>
33. Central Bank of The Bahamas: Project Sand Dollar: About. <https://www.sanddollar.bs/about>, accessed 4 September 2026
34. Chaum, D., Grothoff, C., Moser, T.: How to issue a central bank digital currency. SNB Working Papers 3/2021, Swiss National Bank (Jan 2021), arXiv:2103.00254
35. Chiu, J., Davoodalhosseini, S.M., Jiang, J., Zhu, Y.: Bank market power and central bank digital currency: Theory and quantitative assessment. *Journal of Political Economy* **131**(5), 1213–1248 (2023). <https://doi.org/10.1086/722517>
36. Circles: Circles: A decentralised universal basic income platform based on personal currencies (Retrieved 2021 <https://joincirclesnet/>)

37. Copple, D., Faisal, I., Khairnar, K., Lau, J., Malik, S., Poensgen, V.: The role of holding limits for sterling-denominated systemic stablecoins and a potential digital pound. Financial Stability Paper 53, Bank of England (Nov 2025), <https://www.bankofengland.co.uk/financial-stability-paper/2025/the-role-of-holding-limits-for-sterling-denominated-systemic-stablecoins-and-a-potential-digital>
38. Cúrdia, V., Woodford, M.: The central-bank balance sheet as an instrument of monetary policy. *Journal of Monetary Economics* **58**(1), 54–79 (2011). <https://doi.org/10.1016/j.jmoneco.2010.09.011>
39. Dandekar, P., Goel, A., Govindan, R., Post, I.: Liquidity in credit networks: A little trust goes a long way. In: *Proceedings of the 12th ACM conference on Electronic commerce*. pp. 147–156 (2011)
40. Davoodalhosseini, S.M.: Central bank digital currency and monetary policy. *Journal of Economic Dynamics and Control* **142**, 104150 (2022). <https://doi.org/10.1016/j.jedc.2021.104150>
41. Di Maggio, M., Ghosh, P., Ghosh, S.K., Vats, N., Wu, A.: Central bank digital currency (CBDC), bank deposits, and digital payments: First evidence from a live retail CBDC. NBER Working Paper 32457, National Bureau of Economic Research (2024), <http://www.nber.org/papers/w32457>, revised August 2026
42. Eisenberg, L., Noe, T.H.: Systemic risk in financial systems. *Management Science* **47**(2), 236–249 (2001)
43. Eitan, O., Keidar, I., Shapiro, E.: The grassroots social graph: A secure operating system for multiagent, distributed, peer-to-peer, smartphone-based platforms (2026), in preparation
44. Eitan, O., Keidar, I., Shapiro, E.: Securing people and their machines against major faults (full version). *Proceedings of The 28th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2026)*, to appear (2026), <https://arxiv.org/abs/2607.02304>, arXiv:2607.02304
45. European Central Bank: A stocktake on the digital euro: Summary report on the investigation phase and outlook on the next phase. Tech. rep., European Central Bank (Oct 2023), https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.dedocs231018.en.pdf
46. European Central Bank: Preparation phase of a digital euro — closing report. Tech. rep., European Central Bank (Oct 2025), https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202510.en.html
47. European Parliament and Council: Regulation (EU) no 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (2014), official Journal of the European Union, L 257
48. Fernández-Villaverde, J., Sanches, D., Schilling, L., Uhlig, H.: Central bank digital currency: Central banking for all? *Review of Economic Dynamics* **41**, 225–242 (2021). <https://doi.org/10.1016/j.red.2020.12.004>
49. Fugger, R.: Money as ious in social trust networks & a proposal for a decentralized currency network protocol. Hypertext document. Available electronically at <http://ripple.sourceforge.net> **106** (2004)
50. Garratt, R., Shin, H.S.: Stablecoins versus tokenised deposits: implications for the singleness of money. *BIS Bulletin* 73, Bank for International Settlements (Apr 2023), <https://www.bis.org/publ/bisbull73.pdf>
51. Ghatak, M., Guinnane, T.W.: The economics of lending with joint liability: Theory and practice. *Journal of Development Economics* **60**(1), 195–228 (1999)
52. Glasserman, P., Young, H.P.: Contagion in financial networks. *Journal of Economic Literature* **54**(3), 779–831 (2016)

53. Golike, J., Lewis-Pye, A., Shapiro, E.: Formalising and implementing grassroots social contracts: From legal text to grassroots platforms (full version). arXiv:2609.06231 (2026)
54. Goodfriend, M.: Central banking in the credit turmoil: An assessment of Federal Reserve practice. *Journal of Monetary Economics* **58**(1), 1–12 (2011). <https://doi.org/10.1016/j.jmoneco.2010.09.008>
55. Gopinath, G., Boz, E., Casas, C., Díez, F.J., Gourinchas, P.O., Plagborg-Møller, M.: Dominant currency paradigm. *American Economic Review* **110**(3), 677–719 (2020)
56. Gorton, G.B., Zhang, J.Y.: Taming wildcat stablecoins. *University of Chicago Law Review* **90**(3), 909–971 (2023)
57. Guinnane, T.W.: Cooperatives as information machines: German rural credit co-operatives, 1883–1914. *The Journal of Economic History* **61**(2), 366–389 (2001)
58. Hees, H., Friis, G., Naerland, K., Howitt, A., Kärki, T., Fletcher, A.: Trustlines network white paper (2021, https://doctrustlinesnetwork/assets/pdf/Trustlines_Network_Whitepaper_2021.pdf)
59. Infante, S., Kim, K., Orlik, A., Silva, A.F., Tetlow, R.: Retail CBDC: Implications for banking and financial stability. *Annual Review of Financial Economics* **16**, 207–232 (2024). <https://doi.org/10.1146/annurev-financial-082123-105958>
60. Iosifidis, G., Charette, Y., Airolidi, E., Littera, G., Tassiulas, L., Christakis, N.: Cyclic motifs in the Sardex monetary network. *Nature Human Behaviour* **2**, 822–829 (2018). <https://doi.org/10.1038/s41562-018-0450-0>
61. Karlan, D., Mobius, M., Rosenblat, T., Szeidl, A.: Trust and social collateral. *The Quarterly Journal of Economics* **124**(3), 1307–1361 (2009)
62. Keister, T., Sanches, D.: Should central banks issue digital currency? *The Review of Economic Studies* **90**(1), 404–431 (2023). <https://doi.org/10.1093/restud/rdac017>
63. Kiayias, A., Kohlweiss, M., Sarencheh, A.: PEReDi: Privacy-enhanced, regulated and distributed central bank digital currencies. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*. pp. 1739–1752. ACM (2022). <https://doi.org/10.1145/3548606.3560707>
64. Kim, Y.S., Kwon, O.: Central bank digital currency, credit supply, and financial stability. *Journal of Money, Credit and Banking* **55**(1), 297–321 (2023). <https://doi.org/10.1111/jmcb.12913>
65. Kumhof, M., Noone, C.: Central bank digital currencies — design principles and balance sheet implications. Staff Working Paper 725, Bank of England (May 2018), <https://www.bankofengland.co.uk/working-paper/2018/central-bank-digital-currencies-design-principles-and-balance-sheet-implications>
66. League of Nations: Convention providing a uniform law for bills of exchange and promissory notes. Geneva, 7 June 1930 (1930)
67. Lewis-Pye, A., Naor, O., Shapiro, E.: Grassroots flash: A payment system for grassroots cryptocurrencies. arXiv preprint arXiv:2309.13191 (2023), <https://arxiv.org/abs/2309.13191>
68. Lewis-Pye, A., Shapiro, E.: Volition-guarded multiagent atomic transactions: Describing people and their machines. arXiv preprint arXiv:2604.25596 (2026), <https://arxiv.org/abs/2604.25596>
69. Lovejoy, J., Fields, C., Virza, M., Frederick, T., Urness, D., Karwaski, K., Brownworth, A., Narula, N.: A high performance payment processing system designed for central bank digital currencies. Project hamilton phase

- 1 whitepaper, Federal Reserve Bank of Boston and MIT Digital Currency Initiative (Feb 2022), <https://www.bostonfed.org/-/media/Documents/Project-Hamilton/Project-Hamilton-Phase-1-Whitepaper.pdf>
70. Maimbo, M.S.M., El Qorchi, M.M., Wilson, M.J.F.: Informal Funds Transfer Systems: An analysis of the informal hawala system. International Monetary Fund (2003)
71. Mattsson, C.E.S., Criscione, T., Ruddick, W.O.: Sarafu community inclusion currency 2020–2021. *Scientific Data* **9**, 426 (2022). <https://doi.org/10.1038/s41597-022-01539-4>
72. McLeay, M., Radia, A., Thomas, R.: Money creation in the modern economy. *Bank of England Quarterly Bulletin* **Q1**, 14–27 (2014)
73. Mundell, R.A.: A theory of optimum currency areas. *The American economic review* **51**(4), 657–665 (1961)
74. Olivei, G., Tenreyro, S.: The timing of monetary policy shocks. *American Economic Review* **97**(3), 636–663 (2007)
75. Rogers, J.S.: *The Early History of the Law of Bills and Notes*. Cambridge University Press (1995)
76. Santarosa, V.A.: Financing long-distance trade: The joint liability rule and bills of exchange in eighteenth-century france. *The Journal of Economic History* **75**(3), 690–719 (2015)
77. Selgin, G.A.: *The Theory of Free Banking: Money Supply under Competitive Note Issue*. Rowman & Littlefield, Totowa, NJ (1988)
78. Senn, J., Judmayer, A., Stifter, N., Böhme, R.: Systematization of knowledge: The design space of digital payment systems with potential for CBDC. arXiv:2603.16320 (Mar 2026)
79. Shapiro, E.: Grassroots currencies: A foundation for a grassroots digital economy. arXiv preprint arXiv:2202.05619 (2022), <https://arxiv.org/abs/2202.05619>
80. Shapiro, E.: Glp: A grassroots, multiagent, concurrent, logic programming language for ai (full version). arXiv preprint arXiv:2510.15747, Summary in Proc. of ICLP’26, EPTCS 450, pp. 119–133 (2025), <https://arxiv.org/abs/2510.15747>
81. Shapiro, E.: Grassroots bonds as a foundation for market liquidity. arXiv:2603.13671 (2026), <https://arxiv.org/abs/2603.13671>
82. Tenreyro, S., Thwaites, G.: Pushing on a string: US monetary policy is less powerful in recessions. *American Economic Journal: Macroeconomics* **8**(4), 43–74 (2016)
83. UNCITRAL: *Model law on electronic signatures with guide to enactment* (2001)
84. United Kingdom: Bills of exchange act 1882. 45 & 46 Vict. c. 61 (1882)
85. United Nations Commission on International Trade Law: *UNCITRAL model law on electronic transferable records*. United Nations, New York (2017), https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
86. United States Congress: *Electronic signatures in global and national commerce act* (2000), public Law 106–229, 114 Stat. 464
87. White, L.H.: *Free Banking in Britain: Theory, Experience, and Debate, 1800–1845*. Cambridge University Press, Cambridge (1984)
88. Working Group on E-CNY Research and Development of the People’s Bank of China: Progress of research and development of E-CNY in China. Tech. rep., People’s Bank of China (Jul 2021), <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>
89. World Bank: Remittance prices worldwide quarterly. <https://remittanceprices.worldbank.org> (2025)

90. Wüst, K., Kostiainen, K., Delius, N., Čapkun, S.: Platypus: A central bank digital currency with unlinkable transactions and privacy-preserving regulation. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22). ACM (2022)

A The Grassroots Social Contract, Its Act Schemas and Its Modalities

A grassroots social contract [53] is a finite list of clauses its parties undertake towards one another. A clause that describes an act is written as an *act schema*: the act’s roles, which of them must will it, and the atoms it requires, forbids, adds and deletes at each role. The volition-guarded multiagent atomic transactions [68] realising the contract are compiled from the schemas; three syntactic conditions on the schemas suffice for the protocol so realised to be volitionally grassroots; and each clause is *enforced*, *attested* or *undertaken* by the contract according to what its runs determine and record. This appendix presents the contract in full, writes its clauses as act schemas, identifies the modality of each, and shows the contract syntactically grassroots.

A.1 The Clauses

Definitions. A *party* is a person, natural or legal, with the gender-neutral pronoun “they”, and *Alice*, *Bob* and *Carol* are variables naming distinct parties. A *grassroots coin* names its issuer and its denomination — a fiat currency — and is due now; a *grassroots bond* names a maturity date besides and is due then. *Dollar* names one denomination, and an *Alice Dollar-denominated coin* or *bond*, *Alice-coin* and *Alice-bond* for short, is one issued by Alice. Each party keeps a date. A bond is *mature* when its maturity date is at most the date of its issuer.

The contract.

1. *Minting.* Alice may decide to issue their coins, of any denomination, and their bonds, of any denomination and of a maturity later than their own date.
2. *Date.* Alice keeps their date at the current date and warrants it whenever an Alice-coin is taken for a matured Alice-bond.
3. *Swap.* Alice and Bob may jointly decide to swap Dollar-denominated coins and bonds they hold.
4. *Acceptance.* Alice may decide to accept Carol-coins in payment up to a limit of their choosing, if they hold a Carol-coin or a Carol-bond; each Carol-coin paid to Alice counts against the limit, and Alice may decide again.
5. *Payment.* Alice may decide to pay Bob Dollar-denominated coins they hold that Bob accepts.
6. *Redemption.* Alice may decide to redeem a Bob-coin they hold against any Dollar-denominated coin or bond Bob holds, and to take a Bob-coin for a matured Bob-bond they hold.
7. *Pricing.* Alice prices their offerings in Alice-coins and accepts them in payment at those prices.
8. *Denomination.* An Alice-coin and an Alice-bond are each Alice’s debt of one Dollar, the coin due now and the bond at its date; Alice redeems an Alice-coin on presentation at face value, by a Dollar-denominated coin or bond the bearer accepts or by one Dollar.

9. *Escrow*. Alice may deposit Dollar-denominated coins and bonds with Carol for Bob; Carol and Bob may jointly decide to release them to Bob, and Carol and Alice to return them to Alice, as the agreed condition is met or fails.

Clauses 1–6 and 9 describe acts; 7 and 8 describe none. Clauses 1, 3, 5, 6 and 7 are the contract of grassroots currencies [79] with a bond in place of a coin where the act allows one, clauses 2 and 9 are the date and escrow clauses of grassroots bonds [81], and clauses 4 and 8 are new here. The two are of different kinds: clause 8 denominates, adding the variable f to every act and adding no act, while clause 4 adds the acts accept, payout and spend. Clause 4 is the extension of the contract of grassroots currencies by which a party undertakes to accept named currencies besides their own [79], and with it clause 5 pays coins of the payee, of the payer, or of a third party, who takes part in the payment. A swap in which each party gives coins of their own issue opens a mutual credit line; one in which a party gives coins and the other their own bonds of larger face value maturing later is a loan. Carol in clause 9 is the escrow agent. No clause names the central bank, which as a party is bound by clauses 1–9 like any other. The denomination of a debt is not its governing law: which law governs an obligation, and in which forum it is enforced, are settled outside the contract. A swap across denominations is not an act of the contract: it is two swaps, one in each denomination, or an escrow whose transfers are each in one (Appendix D).

A.2 The Act Schemas

Four predicates. $\mathfrak{c}$, of arity three: $\mathfrak{c}(u, f, d)$ in the state of p is an f -denominated bond issued by u with maturity date d , held by p , and $\mathfrak{c}(u, f, \perp)$ is an f -denominated coin of u , due now; d ranges over $\mathbb{N} \cup \{\perp\}$. *date*, of arity one: *date*(t) in the state of p is the date of p . *dated*, of arity two: *dated*(u, t) in the state of p is u 's warranty to p that their date was t . *accepts*, of arity two: *accepts*(u, f) in the state of p is p 's acceptance of u 's f -denominated coins in payment. The roles are p, q, e and s , the last the issuer of the coins paid in a payment in the coins of a third party; the party variables are u, v and r ; f is the denomination variable, over the countable set $\mathcal{F}$, disjoint from Π ; the numeric variables are d, d' for maturity dates, t, t' for dates, k, k' for amounts, and L for an acceptance limit. The seven clauses that describe acts become twelve schemas, payment taking three, redemption two and escrow three. Nine are the schemas of the undenominated contract [81] with the denomination added — $\mathfrak{c}$ takes the denomination as a middle argument, and every schema carries the one denomination variable f — and three are new here: accept, and the two payments in coins the payee did not issue, payout by their issuer and spend by a holder, with the issuer as a third role.

schema	at its first role	at its second role
$\text{mint}(p?; f, d, k, t) \mid d = \perp \vee d > t :$	$\text{date}(t), +k \cdot \mathfrak{c}(p, f, d)$	
$\text{advance}(p; t, t') \mid t' > t :$	$-\text{date}(t), +\text{date}(t')$	
$\text{swap}(p?, q?; f, u, d, k, v, d', k') :$	$-k \cdot \mathfrak{c}(u, f, d), +k' \cdot \mathfrak{c}(v, f, d')$	$-k' \cdot \mathfrak{c}(v, f, d'), +k \cdot \mathfrak{c}(u, f, d)$
$\text{accept}(p?; f, u, d, L) :$	$\mathfrak{c}(u, f, d), +L \cdot \text{accepts}(u, f)$	
$\text{pay}(p?, q; f, k) :$	$-k \cdot \mathfrak{c}(q, f, \perp)$	$+k \cdot \mathfrak{c}(q, f, \perp)$
$\text{payout}(p?, q; f, k) :$	$-k \cdot \mathfrak{c}(p, f, \perp)$	$-k \cdot \text{accepts}(p, f), +k \cdot \mathfrak{c}(p, f, \perp)$
$\text{spend}(p?, q, s; f, k) :$	$-k \cdot \mathfrak{c}(s, f, \perp)$	$-k \cdot \text{accepts}(s, f), +k \cdot \mathfrak{c}(s, f, \perp)$
$\text{redeem}(p?, q; f, r, d') :$	$-\mathfrak{c}(q, f, \perp), +\mathfrak{c}(r, f, d')$	$-\mathfrak{c}(r, f, d'), +\mathfrak{c}(q, f, \perp)$
$\text{mature}(p?, q; f, d, t) \mid d \leq t :$	$-\mathfrak{c}(q, f, d), +\mathfrak{c}(q, f, \perp), +\text{dated}(q, t)$	$\text{date}(t)$
$\text{deposit}(p?, e?; f, u, d, k) :$	$-k \cdot \mathfrak{c}(u, f, d)$	$+k \cdot \mathfrak{c}(u, f, d)$
$\text{release}(e?, q?; f, u, d, k) :$	$-k \cdot \mathfrak{c}(u, f, d)$	$+k \cdot \mathfrak{c}(u, f, d)$
$\text{return}(e?, p?; f, u, d, k) :$	$-k \cdot \mathfrak{c}(u, f, d)$	$+k \cdot \mathfrak{c}(u, f, d)$

“Dollar-denominated coins and bonds” is the one variable f of every schema, which every atom of the schema carries: no binding of any schema moves instruments of two denominations, which is Corollary 2.4. “If they hold a Carol-coin or a Carol-bond” of clause 4 is that accept requires at p an instrument of the issuer accepted, of the denomination accepted, and “up to a limit of their choosing” is that accept adds L acceptance atoms at p , one of which each coin so paid to p deletes. “Dollar-denominated coins they hold that Bob accepts” of clause 5 is the three schemas of payment: pay, in which the payee q is the issuer, whose acceptance is clause 7; payout, in which the payer p is the issuer, and q deletes $k \cdot \text{accepts}(p, f)$; and spend, in which the issuer is the third role s , requiring nothing, and q deletes $k \cdot \text{accepts}(s, f)$. No payment reads or warrants a date: a coin carries none, and the issuer takes part to countersign the payment and to record it in their log. The reading of the clauses’ other quoted phrases — the guarding roles, the amounts and maturities of mint, the issuer-judged maturity and the date warranty of mature, the unconstrained r and d' of redeem, the bindings of the mutual credit line and the loan, and the two receivers of release and return, fixed by the escrow agreement (Appendix B) — is that of the undenominated schemas [81], with f carried through.

A.3 The Modality of Each Clause

The definitions are [53]’s. A *clause* of a contract is a proposition about the conduct of its parties, kept or breached by that conduct, and a party it names as answerable is its *obligor*; the runs of the protocol realising the contract *determine* the clause if whether it is kept is a function of the run, and a transaction *may breach* it if it occurs in some correct run that breaches it. A transaction is *witnessed against* a party if after it another of its participants holds an atom naming that party. A clause with obligor o is *enforced* if the runs determine it and every correct run keeps it; *attested* if some transaction may breach it and every transaction that may be witnessed against o ; and *undertaken* if no transaction may breach it, the runs do not determine it, and some transaction is witnessed against o or o ’s undertaking is held by another party.

Clauses 1, 3, 4, 5, 6 and 9 are enforced, clause 2 is attested, and clause 7 is undertaken, as for the undenominated contract [81]: an enforced clause permits

an act and obliges nothing beyond it, with the obligations of clauses 5 and 6 self-executing in the schemas — each schema of payment is guarded by the payer and adds the coins at the payee, who accepts them under clause 7 or under clause 4, and redeem is guarded by the bearer and deletes the instrument taken at the issuer; the issuer of the coins spent is a role of spend and not a guard, so they take part and are not asked; the date warranty of clause 2 is given in the course of mature, which adds $\text{dated}(q, t)$ in the state of the bearer, witnessed against the issuer q and legally enforceable on that record — no other schema warrants a date, so mature is the one act that may breach the clause; and the coin a swap adds in another party’s holding is the record of the pricing undertaking of clause 7.

Clause 8 is undertaken. Handing over a unit of a fiat currency is not an act of the contract, so no transaction of it may breach the clause and no run determines whether it is kept; and it is witnessed against the issuer: the coin $\mathfrak{c}(p, f, d)$ in another party’s holding is the record of a debt of one unit of f , enforceable under the law governing the obligation (Section 2.1). The in-kind fulfilment of clause 8 is redeem, enforced, and its fiat fulfilment is performed outside the contract (Section 2.4). No act of the contract asks for a unit of f either: the presentation for a fiat coin and its payment are both outside it, on the record the coin is; what the contract carries is the coin’s return to its issuer, a payment to it.

The sovereign is not a role. Act schemas cannot name a person, and every party begins in the same empty state, so no schema and no clause distinguishes the sovereign of f from any other party [53]: the map σ and the sovereign’s ability to issue fiat coins (Section 2.2), which set it apart, lie outside the contract. The sovereign mints, swaps, accepts, pays and redeems under the same twelve schemas, and its warranty under clause 2 and its undertakings under clauses 7 and 8 are recorded against it as against anyone.

A.4 The Contract Is Grassroots

A contract is syntactically grassroots if it has an unobstructed introductory act, every predicate its acts require has traceable provenance, and every act not willed by all its parties runs only between parties that already record each other — its role graph, with an edge between two roles when one requires an atom of traceable provenance naming the other, is connected; the protocol realising a syntactically grassroots contract is volitionally grassroots [53]. The three conditions are checked for the undenominated schemas in [81], and the argument f is a denomination and names no person, so the check carries to the schemas shared with it unchanged: the swap at the binding of the mutual credit line is the unobstructed introductory act; $\mathfrak{c}$ and dated have traceable provenance, and date names no person; and pay, redeem and mature, guarded by p , require at p a coin or a bond of the counterparty, an atom of traceable provenance naming them. Of the three schemas new here, accept adds $\text{accepts}(u, f)$ at p where u is an argument of the instrument p requires, so accepts has traceable provenance; payout , guarded by p , has q require $\text{accepts}(p, f)$, naming p ; and spend , guarded

by p , has p require a coin of s and q require $accepts(s, f)$, both naming s , so its role graph is connected through the issuer. A payment in the coins of a third party between two parties who do not record each other is therefore an act of the contract only with the issuer as a party, which is the countersignature of Section 2.4.

The contract is therefore syntactically grassroots at every value of its numeric variables. Its schemas carry numeric variables and the denomination variable, each over a countable set, so their instances are a countable set, and the theorem of [53] is for a finite contract; the conclusion for the countable set is through politeness, a condition on transactions and not on schemas, as for grassroots currencies [79].

Lemma A.1 (Amounts, Dates and Denominations). *The transactions of Definition 2.2 are a polite set [53], and the protocol over them is volitionally grassroots.*

Proof. A set of volition-guarded transactions is *polite* if it is open — any two persons can always be brought to a configuration at which some transaction coupling them is enabled — and closed — every transaction enabled at the end of a safe run has all its participants in one instance of that run, or a guard of it in every instance holding one of them; the protocol over a polite set is volitionally grassroots [53]. Both are conditions on the set of transactions, and neither depends on the number of schemas. The checks above are per schema and per binding and hold at every value of the numeric variables, so each instance is a contract of [53] that is syntactically grassroots. Closure quantifies over the runs of the protocol over the whole set, and a run of the union is not a run of a single instance, so it is proved here of the union, as for grassroots currencies [79]. $\mathfrak{c}$, *dated* and *accepts* have traceable provenance in every schema of every instance, and the induction on a run by which [53] proves that no transition puts an edge whose ends lie in different instances uses only the schema inducing the current transition, so it carries to the union unchanged: whenever p holds an atom naming q , p and q lie in one instance of the run. Mint, advance and accept are unary; swap, deposit, release and return are guarded in all their roles; a pay or a redeem enabled between p and q requires p to hold a q -coin, a mature enabled between p and q requires p to hold a q -bond, a payout enabled between p and q requires q to hold $accepts(p, f)$, and a spend enabled over p , q and s requires p to hold an s -coin and q to hold $accepts(s, f)$, so the participants of each already lie in one instance. The union is therefore closed. For openness take any two persons $p \neq q$: each mints one f -denominated coin of their own, by unary transactions, and a swap of the two is then enabled, and it is a transaction of the union. The union is therefore polite, and the protocol over it is volitionally grassroots.

The contract is therefore syntactically grassroots, and the protocol realising it is volitionally grassroots: any group of persons operates it on its own, and two groups become connected only by a swap willed by a member of each.

B Financial Instruments

This appendix presents the financial instruments of grassroots bonds [81], recalled here so that the claim of Section 5.2 rests on the constructions and not solely on the reference. Every transaction of an instrument is over coins and bonds of one denomination (Corollary 2.4), which we leave implicit below; $\mathfrak{c}_{p,d}^k$ is a multiset of k bonds issued by p and maturing at d , and $\mathfrak{c}_p^k$ is a multiset of k p -coins. Every transaction below is a transaction of the contract of Appendix A at a binding, so no instrument adds a construct to the currency; what an instrument adds is the escrow program that fixes what the agent consents to.

B.1 Instruments That Are One Swap

A swap exchanges one lot — coins of one issuer, or bonds of one issuer and maturity — for another, by an act of both parties. Each instrument below is a swap between p and q , specified by the instruments x that p gives and the instruments y that q gives.

1. **Symmetric mutual credit.** $x = \mathfrak{c}_p^k$, $y = \mathfrak{c}_q^k$: each mints and gives the same number of their own coins, and each thereafter holds coins of the other [79].
2. **Asymmetric mutual credit.** $x = \mathfrak{c}_p^{k'}$, $y = \mathfrak{c}_q^k$ with $k' < k$: p charges a premium for credit to q . As coins are redeemable at par, p may redeem at once and keep the premium, so a premium on coins is not interest [79].
3. **Sale of debt.** $x = \mathfrak{c}_r^k$, $y = \mathfrak{c}_q^{k'}$ with $k' < k$: p sells coins of a third person r to q at a discount, which prices p 's doubt about r 's solvency. The debtor r is not a party.
4. **Zero-coupon loan.** $x = \mathfrak{c}_p^{k'}$, $y = \mathfrak{c}_{q,d}^k$ with $k' < k$: the lender p gives coins now, the borrower q bonds of larger face value maturing at d , and the difference is interest for that term. A bond is not presented for redemption, so the loan cannot be recalled; the borrower may repay early, by redeeming the lender's coins against its own bond.
5. **Sale of debt before maturity.** $x = \mathfrak{c}_{r,d}^k$, $y = \mathfrak{c}_q^{k'}$ with $k' < k$: the discount prices the time to maturity as well as the doubt about r .
6. **Forward contract.** $x = \mathfrak{c}_{p,d}^k$, $y = \mathfrak{c}_{q,d}^{k'}$: bonds of the two parties maturing at one date are swapped at inception, so at d each holds a claim on the other of the agreed face value. Between inception and d each party holds the other's debt, so a default in that interval falls on the counterparty, which a forward settled at d does not.

A currency swap and a repurchase agreement are sequences of two swaps; factoring is a sale of debt; a mortgage is a loan with collateral; a bank's time deposit is its bond, and its demand deposit is its coin.

B.2 The Escrow Agent

An escrow agent e holds coins and bonds on behalf of the parties to an escrow agreement and transfers them by its agreed conditions. Each transfer is a transaction between e and the party giving or receiving them, and e is party to every

transfer, so each is made by the consent of e and that party. What e consents to is fixed by the escrow program implementing the agreement: for a date-based condition, by the local date d_e^* of e ; for an event-based condition, by the judgment of e , informed where needed by an *oracle*, an agent the parties agree to trust for the value of a quantity outside the agreement, which attests but holds no instruments and takes no act. An attestation is not a transaction of the contract: the escrow agent judges from what it sees, its own date and the deposits it holds, and an outside event reaches it outside the contract, as the payment of a fiat coin does; the instruments below that rest on an outside event rest on that. The constructions assume that both parties trust e to follow the escrow program and, for event-based conditions, trust e as adjudicator of the condition. An arrangement has a depositor, a beneficiary and e : the depositor transfers coins or bonds to e ; subsequently e either releases them to the beneficiary or returns them to the depositor. We write $\{(a, x), (b, y)\}$ for the exchange in which a gives the instruments x and b gives the instruments y , guarded by a and b ; $y = \emptyset$ makes it a one-sided transfer. The contract has four such transfers: the deposit, the release and the return of clause 9, and the payment of clause 5, which carries only coins the party receiving them accepts. Bonds therefore do not pass one way from one ordinary party to another; a swap has two sides.

An escrow whose agent is a committee, acting when a threshold of its members agree, is not expressible in a model in which every agent is one person [81].

B.3 Instruments That Employ an Escrow Agent

1. **Packaged exchange.** Parties p and q agree the lots X that p gives, the lots Y that q gives, and an establishment window T_0 . *Deposit*: $\{(p, X), (e, \emptyset)\}$ and $\{(q, Y), (e, \emptyset)\}$, one transfer per lot. *Release*: once every lot of both is deposited, $\{(e, Y), (p, \emptyset)\}$ and $\{(e, X), (q, \emptyset)\}$. *Return*: if the window passes with the lots of a party incomplete, e returns every deposited lot to its depositor. All lots change hands or none do, and neither party holds the other's lots before both deposits are complete. It realises the instruments whose sides are several lots:
 - (a) **Balloon loan.** $X = \mathfrak{C}_p^k$; $Y = \bigcup_{j=1}^n \mathfrak{C}_{q,d_j}^{k_j} \cup \mathfrak{C}_{q,d}^k$: coupon bonds at the payment dates and a principal bond at d .
 - (b) **Fixed-payment loan.** $X = \mathfrak{C}_p^k$; $Y = \bigcup_{j=1}^n \mathfrak{C}_{q,d_j}^{k_j}$: bonds with fixed payments k_j at dates d_j .
 - (c) **Interest rate swap.** $X = \bigcup_j \mathfrak{C}_{p,d_j}^{k_j}$, $Y = \bigcup_j \mathfrak{C}_{q,d_j}^{k'_j}$, where p pays fixed amounts k_j while q pays amounts k'_j that vary with a reference rate, attested by an interest-rate oracle. Periodic settlement exchanges realise the net difference at each date.
2. **Term credit line.** A lender p commits to advance up to k coins to a borrower q , with rate ρ on drawn credit, implied by the face values, payment dates $d_1, \dots, d_n$ and expiry T . *Establishment*: p mints k coins and deposits them with e , $\{(p, \mathfrak{C}_p^k), (e, \emptyset)\}$; e tracks the drawn amount k_d , initially 0. *Draw*: when q draws $k' \leq k - k_d$, q mints a principal bond $\mathfrak{C}_{q,T}^{k'}$ and coupon bonds $\mathfrak{C}_{q,d_j}^{\rho k'}$,

with $\rho k'$ an integer in the smallest unit (Definition 2.1), for each $d_j > d_e^*$ and deposits them with e ; e releases them to p and releases $\mathfrak{c}_p^{k'}$ to q , and k_d becomes $k_d + k'$. *Repayment*: q acquires p -coins and redeems them from p against its principal bond, which p cannot refuse; p deposits them with e , and k_d falls by that amount. The coupon bonds of a repaid draw stand, being q 's debts already issued and held by p . *Expiry*: once $d_e^* \geq T$, e returns the undrawn balance to p . Between the operations of the agreement e holds $\mathfrak{c}_p^{k-k_d}$, and p holds $\mathfrak{c}_{q,T}^{k_d}$ together with the coupon bonds of the draws, with $0 \leq k_d \leq k$, so q cannot draw beyond the limit and the principal p holds equals the amount drawn [81].

3. **Collateral.** To collateralise a loan from p to q : *deposit* $\{(q, x), (e, \emptyset)\}$, the borrower's bonds x to e ; *release on default* $\{(e, x), (p, \emptyset)\}$; *return on fulfilment* $\{(e, x), (q, \emptyset)\}$. The lender of last resort of Section 5.3 lends against such a deposit.
4. **Guarantee.** A guarantor g covers the obligations of q to p : *deposit* $\{(g, \mathfrak{c}_g^k), (e, \emptyset)\}$; *invocation on default* $\{(e, \mathfrak{c}_g^k), (p, \emptyset)\}$; *release on fulfilment* $\{(e, \mathfrak{c}_g^k), (g, \emptyset)\}$.
5. **Option.** An option grants p the right, and not the obligation, to execute a specified swap with q within an exercise window $[d_1, d_2]$ agreed at establishment and judged by d_e^* , with an establishment window T_0 before which both parties must deposit. *Establishment*: p deposits the premium $\mathfrak{c}_p^k$ with e and q deposits the underlying bonds y ; if only one deposits by T_0 , e returns that deposit. *Exercise*: while $d_1 \leq d_e^* \leq d_2$, p may signal exercise, whereupon e releases y to p and the premium to q . *Expiry*: once $d_e^* > d_2$ with no exercise, e returns y to q and transfers the premium to q . American exercise is the window $[0, d]$ and European exercise the window $[d, d_2]$; a window is needed because advance-date is unguarded and may raise d_e^* past d without equalling it. This is a call option; a put option is symmetric, q depositing the strike price and p the bonds it wishes to sell. A strike price is incorporated by a further deposit of p at establishment, released to q on exercise and returned to p on expiry.
6. **Insurance.** The insured p pays a premium and the insurer q a payout if a specified event occurs by expiry T , as e attests. *Establishment*: $\{(q, \mathfrak{c}_q^{k'}), (e, \emptyset)\}$, the insurer's reserve, $k' \gg k$. *Premium*: $\{(p, \mathfrak{c}_p^k), (e, \emptyset)\}$. *Claim*: $\{(e, \mathfrak{c}_q^{k'}), (p, \emptyset)\}$ and $\{(e, \mathfrak{c}_p^k), (q, \emptyset)\}$. *Expiry with no claim*: e transfers the premium to q and returns its reserve. A mutual insurance arrangement is each member depositing premiums into a shared escrow reserve.
7. **Credit default swap.** p pays periodic premiums to the protection seller q , who compensates p if a reference person r defaults, as e adjudicates. *Establishment*: $\{(q, \mathfrak{c}_q^K), (e, \emptyset)\}$, the seller's reserve. *Premium payments*: $\{(p, \mathfrak{c}_{p,d_j}^{k_j}), (e, \emptyset)\}$ at the dates d_j , forwarded to q . *Credit event*: $\{(e, \mathfrak{c}_q^K), (p, \emptyset)\}$. *No credit event*: the premium bonds go to q , and at expiry T the reserve returns to q .
8. **Letter of credit.** A bank b guarantees payment to the seller p on behalf of the buyer q , e verifying that the contractual conditions are met. *Is-*

suance: $\{(b, \mathbb{C}_b^k), (e, \emptyset)\}$. *Presentation*: once e verifies that p has fulfilled the terms, $\{(e, \mathbb{C}_b^k), (p, \emptyset)\}$. *Reimbursement*: the buyer deposits its bonds with e , $\{(q, \mathbb{C}_{q,d}^k), (e, \emptyset)\}$, and e releases them to the bank, $\{(e, \mathbb{C}_{q,d}^k), (b, \emptyset)\}$; the buyer cannot transfer them to the bank directly, there being no such act.

C The Sovereign Market, as It Runs

The denominated acts are a separate program, derived from the bond agent with the denomination as the middle argument of the coin (Section 2.4). Its village is the village market of grassroots bonds [81] — Alice the baker, Bob the farmer, Charlie the carpenter, Diana the doctor, Eve the teacher, Frank the fisherman, and an escrow agent — denominated in one fiat currency, with the central bank as an eighth party and Diana as the community bank. Each party runs the same agent under eight of the nine schemas of grassroots bonds, denominated, and no clause names the central bank.

Below is the output of one run, elided to the transactions this paper rests on. A holding is a list of lots, each naming its issuer, its denomination, its maturity date and its number of instruments, so `lot(cb, usd, 0, 30)` is thirty sovereign grassroots coins: the program has no separate coin and represents one as a bond of maturity 0, where Definition 2.1 has two instruments and a coin carries no date. An `opened(q)` line records a conversation with q that the play has opened: two parties transact over the root channel of a conversation and over nothing else.

```
[CERTIFICATE REFUSED] sovereign reaches the network or the person:
      village:log/2 calls send_to_user/1
tagged(cb, opened(diana))
tagged(diana, opened(cb))
...
tagged(cb, minted(30, 0))
tagged(cb, holdings([lot(cb, usd, 0, 30)]))
...
tagged(diana, swap_done(cb))
tagged(cb, swap_done(diana))
tagged(diana, holdings([lot(cb, usd, 0, 10)]))
tagged(cb, holdings([lot(cb, usd, 0, 20), lot(diana, usd, 0, 10)]))
...
tagged(diana, presented(frank, cb, 0))
tagged(frank, holdings([lot(diana, usd, 0, 6), ...]))
tagged(frank, redeemed(diana, cb, 0))
tagged(frank, warranty(diana, 0))
tagged(frank, holdings([lot(diana, usd, 0, 6), ..., lot(cb, usd, 0, 1)]))
tagged(diana, holdings([lot(cb, usd, 0, 9), ...]))
...
tagged(cb, fiat_paid(frank, 1))
tagged(frank, fiat_received(cb, 1))
tagged(cb, holdings([lot(cb, usd, 0, 21), lot(diana, usd, 0, 10)]))
```

What the run shows. The central bank mints thirty coins of its own and opens a mutual credit line with the community bank: a swap of ten of its coins for ten of hers, at par, on demand and without interest, willed by both, after which each holds coins of the other (Section 4.2). Frank, a household, holds Diana-coins and Diana holds central bank coins, so the f -coin holding graph has the path $frank \rightarrow diana \rightarrow cb$ and after one redemption along it Frank holds a sovereign grassroots coin, which is Proposition 4.3 performed (Section 4.3). Diana warrants her date in that transaction: the program gives the warranty in every payment and redemption, where clause 2 requires it when a matured bond is taken for a coin. Frank then presents the sovereign coin to the central bank and is paid one unit of the fiat currency: the coin returns to its issuer by a payment to it (Definition 2.2), its coins in circulation fall by one, and the payment of the fiat unit is outside the contract, which carries no act for it (Appendix A).

What the run does not show. The engine refuses the certificate of the program this village play belongs to, because the play prints to the person; the denominated agent itself is a certified mini-app, as the grassroots currencies agent is (Section 2.4). Mature, accept, payout and spend are not implemented either. Throughput, deployed scale and ease of use are unmeasured, here as elsewhere.

D Exchange across Denominations

Persons can exchange grassroots coins across denominations among themselves, with no bank accounts and no correspondent banking. Coins of any two denominations can be exchanged directly, so the exchange may bypass the vehicle currency of today's markets: the US dollar, the vehicle of foreign exchange and the invoicing currency of commodities [55].

Exchange as paired payments. A person p holding Dollar-denominated grassroots coins and a person q holding Euro-denominated ones agree a rate and exchange by a pair of payments: p pays q x Dollar-denominated coins acceptable to q , and q pays p y Euro-denominated coins acceptable to p , each payment a transaction of one denomination (Section 2.1). The rate y/x is set by the parties: the architecture neither performs nor constrains conversion (Corollary 2.4), and rates are set by competition among the persons quoting them. The two payments are separate transactions, so one party is exposed between the legs; the exposure is bounded by exchanging coin by coin, or by the mutual credit the parties extend each other.

Escrowed exchange. The escrow agent of grassroots bonds (Appendix B) holds coins and bonds on behalf of the parties and transfers them by its conditions, and every deposit, release and return is a transfer of instruments of one denomination, so escrow composes with denomination. An exchange agreement: p deposits x Dollar-denominated coins with the escrow agent e , q deposits y Euro-denominated ones, and e releases the two deposits crosswise, or returns a lone deposit if the other is not made within the establishment window. Both legs complete or neither, at the end of the agreement: the parties need no mutual

credit and no trust in each other, only in e . The agreement is not one transaction — no transaction spans two denominations (Corollary 2.4) — so between the two releases there is a state in which one leg has completed and the other has not; the escrow agent guarantees the outcome of the agreement, and in that state each party's exposure is to e . Forwards and options across denominations are the escrow instruments of [81] with legs in distinct denominations, each transaction within one denomination.

Consequences. A person holding grassroots coins of several denominations, quoting rates and standing ready to exchange, is a money changer, and competition among money changers sets the rates. A migrant worker can exchange into the home denomination and pay family directly, avoiding the correspondent-banking chain and its fees [89], though a money changer, an issuer or an escrow agent may charge a spread or a fee. A person with assets in one denomination and a liability in another covers by exchange, bearing the rate risk. Exchange, remittance and covering thus proceed among persons, in legally binding debts of the fiat units, without correspondent banking.