Grassroots Currencies: Turning Mutual Trust into Liquidity (Full Version)

Ehud Shapiro

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

Abstract. Global cryptocurrencies such as Bitcoin and Ether are unbacked and bear the cost of global consensus on every transaction. A grassroots coin is a claim on its issuer—any person, natural or legal, including people, communities, cooperatives, corporations, banks, municipalities and governments—who undertakes to accept their own coins for their offerings at the prices they post, and a transaction costs no more than operating a smartphone. A grassroots coin is a unit of its issuer's debt, which the issuer must redeem at par (1-for-1) against any grassroots coin they hold. Liquidity arises from mutual credit lines, formed by the voluntary swap of coins among persons who know and trust each other; coin redemption pegs mutually-liquid currencies at par and carries payments along chains of holdings.

Here, we specify grassroots currencies by a grassroots social contract written in natural language (English), present its properties, and show two realisations of it: with pen-and-paper coins, and by formalising the contract and compiling it down an abstraction cascade to a working smartphone app. The implementation works: six agents running the compiled program carry out a village market of swaps, payments and redemptions, and the app shows each villager the holdings the scenario prescribes.

The contract specifies four transactions—mint, swap, pay, redeem—and the coins in circulation form a directed multigraph, one edge per coin from its holder to its issuer, on which a redemption may act. The monetary properties of grassroots currencies are then properties of that graph. We prove that grassroots currencies are volitionally grassroots—any group may operate on its own, and two groups become connected only by a meeting willed by both; adapt the classical liquidity ratios and creditworthiness measures to grassroots coins; and prove that a community clears its debts into a designated member, in any order and with no coordination, exactly when no other member owes more grassroots coins than they hold, that the number of coins of that member a group can obtain by its own redemptions is the maximum flow from the group to that member in the graph of holdings, and that a redemption run on a person is met in full exactly when they hold at least as many coins as they owe.

Grassroots currencies may thus allow local digital economies to form and grow without initial capital or external credit, harnessing mutual trust within communities into liquidity, operating solely on the networked smartphones of their members, merging gradually into a global digital economy, and helping 'banking the unbanked'.

1 Introduction

Grassroots currencies. Global cryptocurrencies such as Bitcoin [67] and Ether [12] are unbacked and bear the cost of global consensus on every transaction. A grassroots coin is a claim on its issuer—any person, natural or legal, including people, communities, cooperatives, corporations, banks, municipalities and governments—who undertakes to accept their own coins for their offerings at the prices they post, and a transaction costs no more than operating a smartphone.Grassroots currencies are similar to fiat currencies in that scarcity is controlled by the issuer rather than by a protocol, in contrast to global cryptocurrencies such as Bitcoin [67] or Ethereum [12]. They are similar to 'inside money' [14,15]—a medium of exchange backed by private credit—in that they are backed by claims on the issuer.

Grassroots platforms are person-to-person smartphone apps that realise Proudhon's two-centuries-old notion of a social contract that can have multiple independent instances that may coalesce by mutual consent, possibly into a single global instance [72,85,87]; grassroots currencies are one. Grassroots currencies aim to provide a foundation for grassroots digital economies, allowing them to emerge without initial capital or external credit, operating solely on the networked smartphones of their members, and gradually merge into a global digital economy. As such, grassroots currencies may, by harnessing mutual trust within communities, help 'banking the unbanked' [2,10]. These abilities may be most relevant where capital and external credit are scarce while trust within families and communities is not.

Value and redemption. Grassroots currencies are endowed with value by their issuer undertaking to redeem them against their offerings: Goods and services for people and corporations; interest and transaction fees for banks; and taxes for cities and states. Critically, the offerings of each person include all the grassroots coins they hold, including coins issued by other persons. A grassroots coin is a unit of its issuer's debt, which the issuer must redeem at par (1-for-1) against any grassroots coin they hold.

Coin redemption is key for a digital economy based on grassroots currencies to function, as it (*i*) makes coins issued by the same person fungible; (*ii*) resolves double spending [57]; (*iii*) allows credit to be settled and extinguished; (*iv*) allows chain payments across mutually-liquid currencies; and (*v*) prices mutually-liquid grassroots currencies at par, while their issuers meet presentations.

Liquidity through mutual credit. As each person prices their goods and services in terms of their own currency, trade is impossible if no person holds another person's coins. Liquidity arises from mutual credit lines, formed by the voluntary swap of coins among persons who know and trust each other; coin redemption pegs mutually-liquid currencies at par and carries payments along chains of holdings. Such persons are family members, friends, peers, and colleagues; a community bank and its members; a corporation and its owners, employees, suppliers, and customers; philanthropic organisations, their donors, and the persons they support; a municipality and its local businesses. Liquidity is correlated with the amount and distribution of coins in circulation. A grassroots

coin in circulation is an outstanding obligation by its issuer to its holder, and the coins in circulation in a digital economy record the credit its members have extended one another. The count itself is no measure across persons, each pricing their offerings in units of their own choosing. Since grassroots coins are redeemed at par, mutual credit is also at par: a credit line opened with a premium for one party can be closed by that party at once, keeping the premium. Interest-bearing credit therefore needs a second instrument beside the coin. A grassroots bond is a debt of its issuer with a date, and its bearer redeems it against coins once that date has come. Bonds are the subject of a separate paper [90].

Specification by a grassroots social contract. Here, we specify grassroots currencies by a *grassroots social contract* [37] written in natural language (English), present its properties (Section 2), and show two realisations of it: with pen-and-paper coins (Figure 1, Section 3), and by formalising the contract and compiling it down an abstraction cascade to a working smartphone app (Section 4). The clauses of the contract are what its parties undertake towards one another: minting, swap, payment, redemption, and pricing. The contract extends the base contract of grassroots keys and knowledge [37], by which persons establish their identities and come to know one another: a swap is between persons who know each other, and a payment or a redemption is to a person the payer knows. A grassroots social contract is a social contract meeting Proudhon's conditions—reciprocal, imposing no obligation upon the parties except that which results from their personal promise, subject to no external authority, freely accepted and signed by all the participants—and two more, that people are free to deal with each other and that there is no external register of people. A contract meeting these conditions has the property he envisioned: any two people may come into relation without anyone's leave, two communities that adopted the contract independently can later become one, and every participant in an act is a party [37].

While the intended realisation of grassroots currencies is digital, the abstract contract does not dictate that. Hence, we first illustrate the contract and its implications via a pen-and-paper realisation. This simplifies their exposition and uncovers their inherent properties as a currency (Section 3): a paper coin is a signed undertaking analogous to a promissory note, its obligations those of an ordinary contract, and a swap of coins at a meeting is physically atomic.

From the contract to the app. Down the abstraction cascade [93] to the program every participant runs, the clauses become act schemas; the schemas compile to volition-guarded multiagent atomic transactions [58], each guarded by the persons whose consent it takes; and the transactions become the clauses of a program in vGLP [93], compiled to GLP [89], a multiagent concurrent logic programming language running on Dart for smartphone deployment. The Grassroots Super-App [26] runs grassroots platforms as mini-apps, each a certified program it installs and activates and whose interface it renders, and grassroots currencies is one of them. The contract is implemented, and the implementation works: a six-agent village market run on the compiled program exercises mutual credit, payments, swaps, redemption, and the sale of debt, and the app compiled from the contract shows each villager the holdings the scenario

prescribes (Appendix B, Figure 8). The results of this paper are theorems about the transactions, so they hold under both realisations, on paper and digitally.

From the currency to its graph. The contract specifies four transactions—mint, swap, pay, redeem—and the coins in circulation form a directed multigraph, one edge per coin from its holder to its issuer, on which a redemption may act. The monetary properties of grassroots currencies are then properties of that graph. A coin an issuer holds of their own carries no value and no edge, so minting adds none; a swap of coins the two parties have issued adds an edge each way between them; a payment deletes an edge; and a redemption deletes the bearer's edge to the issuer and moves one of the issuer's edges to the bearer. The out-degree of a person is the coins of others they hold, and their in-degree is the coins of theirs that others hold. A community clears its debts into a designated member exactly when every other member's out-degree is at least their in-degree. The coins of that member a group can obtain by its own redemptions are the maximum flow from the group to it. A redemption run on a person is met in full exactly when the coins they hold cover the coins they owe. The contract determines the transactions, the transactions determine the holdings, and these properties are read from the degrees and the maximum flows of the graph of holdings.

Grassroots, solvency, liquidity, and runs on the bank. We prove that grassroots currencies are volitionally grassroots—any group may operate on its own, and two groups become connected only by a meeting willed by both (Section 4). We adapt the classical liquidity ratios and creditworthiness measures to grassroots coins—the liquidity ratios of corporate finance and the creditworthiness measures of international monetary economics—introduce the community bank, and prove that a community clears its debts into a designated member, in any order and with no coordination, exactly when no other member owes more grassroots coins than they hold, that the number of coins of that member a group can obtain by its own redemptions is the maximum flow from the group to that member in the graph of holdings, and that a redemption run on a person is met in full exactly when they hold at least as many coins as they owe—properties of the graph of holdings, needing no coordination among the persons (Section 2.5). Grassroots currencies may thus allow local digital economies to form and grow without initial capital or external credit, harnessing mutual trust within communities into liquidity, operating solely on the networked smartphones of their members, merging gradually into a global digital economy, and helping 'banking the unbanked' [2,10].

Paper structure. Section 2 presents the grassroots currencies social contract and its properties. Section 3 presents their pen-and-paper realisation. Section 4 presents their digital realisation. Section 5 presents the economics of grassroots currencies, assuming them broadly deployed. Section 6 places the work among related work, and Section 7 concludes. The appendices carry act schemas of the contract (A); program and the village market (B); the proofs (C); more on liquidity (D); economic scenarios (E); more on the digital realisation (F); implementation notes (G); and related work, continued (H).



Fig. 1. Pen-and-paper grassroots currencies. **A.** Four persons, each with a pile of grassroots paper coins they have minted, each pricing their offerings in their own coins; no trade is possible, as no person holds another's coins. **B.** Mutual credit lines formed by voluntary swaps of grassroots paper coins among neighbours; trade can commence. **C.** The blue person has paid a green coin to the green person for a green tea bag.

2 Grassroots Currencies and Their Properties

Here we specify grassroots currencies by a social contract [37] and analyse their properties.

2.1 The Grassroots Currencies Social Contract

The grassroots currencies social contract [37] below describes what parties undertake towards one another. A *party* is a person, natural or legal (with the gender-neutral pronoun 'they'), with *Alice*, *Bob* and *Carol* as variables naming distinct parties to the contract. A *grassroots coin* is a unit of debt that names its issuer, with *Alice-coin* referring to a grassroots coin issued by Alice. The contract extends GKK, the grassroots keys and knowledge contract [37], whose clauses it cites and does not restate: a person establishes their identity by choosing their own key pair, and makes themselves known by the public key (GKK:1); two persons may come to know each other by an act of both (GKK:2); and a person who knows two persons may introduce one to the other, by an act of the introducer and the one introduced to (GKK:3). A person *knows* another when they hold the other's public key; a coin carries its issuer's public key, so whoever holds one knows its issuer. Each clause opens with its legal modality [37]: ■ *enforced*, no act of the contract can breach it; ○ *undertaken*, its performance lies outside the contract, which records only the undertaking (Appendix A.2). The box ends with the contract's *pragmas*, which the app compiled from the contract follows [37]: a tab of the app and what it lists, and for each clause the person proposing an act, the button in brackets, pressed in the row of the person who takes the act's other role, a field in angle brackets for each variable of the act's schema, and, indented, each person asked with the question put to them.

GC: Grassroots Currencies

Alice and Bob are persons.

1. ■ *Minting.* Alice may decide to issue Alice-coins.
2. ■ *Swap.* Alice and Bob, who know each other, may jointly decide to swap coins they hold.
3. ■ *Payment.* Alice may decide to pay Bob-coins they hold to Bob, whom they know.
4. ■ *Redemption.* Alice may decide to redeem a Bob-coin they hold against any coin held by Bob, whom they know.
5. ○ *Pricing.* Alice prices their offerings in Alice-coins and accepts them in payment at those prices.

Pragmas

Coins: the coins Alice holds.
Minting: `Alice [Mint] <amount>`
Swap: `Alice [Swap] <issuer given> <amount given> <issuer wanted> <amount wanted>`
`Bob: Alice asks to swap coins with you.`
Payment: `Alice [Pay] <amount>`
Redemption: `Alice [Redeem] <issuer wanted>`

2.2 The Transactions

We assume a potentially infinite set of persons Π and consider only finite subsets of it; a grassroots p-coin, denoted $¢_p$, is a unit of debt issued by $p \in \Pi$, and $¢_p^k$ is a multiset of k coins $¢_p$. Each agent is a person operating a machine, and here the machine state of a party p is their holdings c_p, a multiset of coins, initially empty, and the set $K_p \subseteq \Pi$ of the persons p knows, initially empty, which the transactions of GKK [37] add to, and to which a transaction below that gives p a coin of issuer u adds u, a coin carrying its issuer's public key; K_p is the set of persons the *knows* atoms of p's state name (Appendix A), an atom added again or naming p changing it not at all. 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. Transactions that differ only in the configurations are *equivalent*. A run is *safe* if every step is a transaction of the protocol. We use $\cup$ and $\setminus$ for multiset sum and difference. The four transactions are the following.

Definition 2.1 (The Transactions of Grassroots Currencies). *For persons $p \neq q \in \Pi$, $u, v, r \in \Pi$ and amounts $k, k' \geq 1$, the **transactions of grassroots currencies** are the volition-guarded transactions $(c \to c', Q')$ below, Q' their guards [58], over the participants named, in which c satisfies the precondition stated, a participant who receives a coin of issuer u has $K'_p = K_p \cup \{u\}$, and $c'_x = c_x$ for every person x not named:*

1. ***Mint**$_p(k)$, over $\{p\}$, guarded by $\{p\}$: $c'_p = c_p \cup ¢_p^k$.*
2. ***Swap**$_{p,q}(¢_u^k, ¢_v^{k'})$, over $\{p, q\}$, guarded by $\{p, q\}$, with $u \neq v$: precondition $q \in K_p$, $p \in K_q$, $¢_u^k \subseteq c_p$ and $¢_v^{k'} \subseteq c_q$; $c'_p = c_p \setminus ¢_u^k \cup ¢_v^{k'}$ and $c'_q = c_q \setminus ¢_v^{k'} \cup ¢_u^k$.*
3. ***Pay**$_{p,q}(k)$, over $\{p, q\}$, guarded by $\{p\}$: precondition $q \in K_p$ and $¢_q^k \subseteq c_p$; $c'_p = c_p \setminus ¢_q^k$ and $c'_q = c_q \cup ¢_q^k$.*
4. ***Redeem**$_{p,q}(r)$, over $\{p, q\}$, guarded by $\{p\}$, with $r \neq q$: precondition $q \in K_p$, $¢_q \in c_p$ and $¢_r \in c_q$; $c'_p = c_p \setminus ¢_q \cup ¢_r$ and $c'_q = c_q \setminus ¢_r \cup ¢_q$.*

***Equivalence** is the least equivalence on the underlying machine transactions under which two transactions with the same name and arguments, differing only in the configurations c and c', are equivalent.*

Mint, pay, and redeem are guarded by the initiator; a swap is guarded by both parties. A redemption is also the swap of the same two coins, so the two are equivalent, and their class is guarded by the bearer; p's q-coin taken for q's p-coin is a redemption by either of them, so its class is guarded by either. These transactions, with those of GKK, which add to the sets K_p and touch no coin, define a grassroots currencies protocol GC [58], with the following property.

Lemma 2.2 (Conservation of Money, [58] for coins). *In any safe run r of GC, the p-coins in any configuration $c \in r$ are exactly the p-coins minted by p in the prefix of the run ending in c.*

Lemma 2.3 (Knowledge of the Issuer). *In any safe run of GC, a person who holds a coin of another issuer knows that issuer.*

Proof. Initially every holding is empty. Mint and pay give a person coins of their own issue; swap and redeem give a participant coins of an issuer u and add u to that participant's K; and no transaction removes a person from a K.

2.3 The Graph of Holdings

The holdings of a grassroots economy form a directed multigraph, one edge per coin from its holder to its issuer, and that graph is the object of this section: the out-degree of a person is the coins of others they hold, their in-degree is the coins of theirs that others hold, and a redemption against a coin of another issuer shortens a path: where p holds a q-coin and q an r-coin, $r \neq q$, the two edges $p \to q \to r$ become the one edge $p \to r$, the q-coin returning to q, and where $r = p$ the two-cycle disappears by set-off. Every such rewrite leaves the out-degree minus the in-degree of every person unchanged, and that invariant is what the results below rest on. The persons act independently, each by their own rights, so we state and prove the answers in graph terms: the holdings form a graph, solvency depends on the graph degrees, and liquidity on the graph maximum flows. No participant sees this graph; each sees their own holdings and what others disclose to them. It is a mathematical construction for analysing the currency.

2.4 Assets, Liabilities, and the Liquidity Ratio

Let $\nu(p, q)$ be the number of q-coins held by p, where $p \neq q$ (zero if $p = q$, as p-coins held by p carry no value). The *assets* of p are the coins of other issuers they hold, $a_p := \sum_q \nu(p, q)$, and their *liabilities* are their coins in circulation, $\ell_p := \sum_q \nu(q, p)$. The *liquidity ratio* of p is a_p/ℓ_p, undefined when $\ell_p = 0$.

A person is *insolvent* when their liabilities exceed their assets, $a_p < \ell_p$: not every coin of theirs in circulation can be redeemed for a coin of another issuer, and no redemption of their own remedies that, as we prove below.

2.5 Solvency, Liquidity, and Runs on the Bank

Computations. A *configuration* records, for every person, their holdings and the persons they know; a *transition* leads from one configuration to the next—a transaction of the contract (Section 2) taking place. A *computation* is a sequence of configurations, each reached from the previous by a transition; it is *safe* if every step is one, and a transaction is *enabled* in a configuration if its preconditions hold there. The possibility results below (Propositions 2.7 and 2.11) quantify over safe computations—what can happen; the liveness results (Propositions 2.8 and 2.13) quantify over computations in which persons act on their rights—persons who can redeem do (Definition 2.6)—and state what must then happen. In the volitional framework [58], liveness takes an enabled class that is willed by its guards (Section 4.2); that a bearer wills an enabled redemption is an assumption about persons, under both realisations. The proofs of the propositions below are in Appendix C.

Chain redemption. Chain redemption allows trade among parties that are connected in the holding graph, even if not adjacent.

Proposition 2.4 (Chain Redemption). *Let $p_0, p_1, \ldots, p_k$ be a sequence of distinct persons with $k \geq 1$ such that each p_i ($0 \leq i < k$) holds a 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 a p_k-coin.

A chain of holdings from p to q—each person holding a coin of the next—is a chain of mutual liquidity: by Proposition 2.4, a sequence of redemptions along the path leaves p holding a q-coin. Concurrent redemption chains that need the same coin interfere; what a group of persons can obtain by such chains is exactly the maximum-flow bound of Proposition 2.11.

Graph solvency. Can a community extinguish all its internal debts? A debt is extinguished when the coin returns to its issuer, and a redemption does exactly that: the holder returns a coin to its issuer and takes in exchange any coin the issuer holds—as of right, the issuer being bound to redeem on presentation (Section 2), without transferring value, and without changing any person's assets net of liabilities. 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. The results are stated relative to a designated person $s \in \Pi$, the **sink**: the member with whom the community's net position is left—the community bank of Section 5.3, or any member so designated. Here we define the debts of a community as a graph, one edge per coin from holder to issuer, and prove: the community can extinguish all its debts into the sink by redemptions exactly when every member but the sink holds at least as many coins as they owe (Proposition 2.7); and when it can, every maximal computation of clearing redemptions among its members ends with them cleared, in any order and with no coordination (Proposition 2.8). Clearing uses Redeem: a Pay transfers value and a swap requires the counterparty's consent.

Definition 2.5 (Holding Graph, Sink-Closed). *Given a configuration and a designated person $s \in \Pi$, the **sink**, the **holding graph** G is the directed multigraph with the persons as vertices and an edge $u \to v$ for each v-coin that person $u \neq v$ holds. A set of vertices containing s is **sink-closed** if every edge between two vertices other than s has both endpoints in the set or neither.*

The out-degree and in-degree of p in G are their assets a_p and liabilities ℓ_p. A sink-closed set of persons is a community whose only claims across its boundary are with the sink; the sink is a member of every such community. A Redeem transaction in which the debtor is not s and the coin taken is not issued by the debtor is a *clearing redemption*.

Definition 2.6 (Clearing into the Sink, Complete Clearing, Maximal). *Given a configuration and a sink-closed set V of the holding graph, the holdings of V **clear into** s if some finite safe computation of clearing redemptions among members of V leads to a configuration in which every coin of an issuer in V other than s is held by its issuer, and **clear completely** if it leads to one in which every coin of an issuer in V is held by its issuer. A finite safe computation of clearing redemptions among members of V is **maximal** if no clearing redemption among members of V is enabled in its last configuration.*

Proposition 2.7 (Graph Solvency). *The holdings of a sink-closed set V clear into s if and only if $a_p \geq \ell_p$ for every member p of V other than s, and cleared holdings leave each such member holding exactly $a_p - \ell_p$ coins of the sink.*

Proposition 2.8 (Clearing Liveness). *If $a_p \geq \ell_p$ for every member p of V other than s, then every maximal computation of clearing redemptions among members of V ends with the holdings of V cleared into s, after at most $\sum_{p \in V \setminus \{s\}} \ell_p$ redemptions.*

Maximality assumes that members persistently will a clearing redemption while one is available; in a correct digital run an enabled transaction its guards will is eventually taken (Appendix B), and whether a person wills it is theirs. Complete clearing is the case of equality throughout, and the special cases of Proposition 2.7 are in Appendix D.

Corollary 2.9 (Complete Clearing). *The holdings of all persons clear completely if and only if $a_p = \ell_p$ for every person.*

Proof. If $a_p = \ell_p$ for every person, then for any designated sink s the holdings clear into s by Proposition 2.7, and each member other than s then holds $a_p - \ell_p = 0$ coins of the sink, so no coin of s is held by another and every coin is held by its issuer. Conversely, in completely cleared holdings $a_p = \ell_p = 0$ for every person, and $a_p - \ell_p$ is invariant under Redeem (Appendix C), so $a_p = \ell_p$ in the given configuration.

Graph liquidity. For clearing, any coin of the debtor may be taken; here a group needs specifically coins of the sink—s-coins. How many can it obtain by its own redemptions? Each redemption exchanges a coin the redeemer holds for a coin of the coin's issuer, so a member holding a coin whose issuer holds a coin whose issuer holds a coin, and so on to the sink, obtains an s-coin by chain redemption (Proposition 2.4), consuming the coins along the chain. Two chains that need the same coin cannot both complete, so the group obtains one s-coin per chain, over chains that share no coin; the maximum number of such chains is a maximum flow in the holding graph. We recall the max-flow min-cut theorem [29,33,63]: in a finite directed multigraph with unit edge capacities, the maximum flow from a set of source vertices to a sink vertex is realised by a maximum-size set of pairwise edge-disjoint directed paths from sources to the sink, and equals the minimum, over sets S of vertices containing the sources and not the sink, of the number of edges from S to its complement—a *cut*.

Definition 2.10 (Group Liquidity). *Given a configuration and a set A of persons not containing s, the **liquidity of** A is the maximum, over finite safe computations of Redeem transitions of members of A from the configuration, of the number of s-coins members of A hold in the last configuration.*

Proposition 2.11 (Graph Liquidity). *The liquidity of A is the maximum flow from A to s in G.*

The edges here 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. For a single person, $A = \{p\}$, the proposition states what they can obtain by themselves: their out-degree in G counts the coins they hold—the numerator of their liquidity ratio—and the maximum flow is the number of s-coins they can reach by redemptions. The proposition concerns unilateral capacity, what the members can obtain by

their own rights, now: the transactions of persons not in A are outside their control. Group liquidity is subadditive, as paths of different members share edges.

Redemption runs. In a redemption run, the "run on the bank" of banking, the holders of a person's coins present them all at once, and the person meets each presentation with a coin they hold. Each fulfilled presentation returns one p-coin to p and takes one coin from p's holdings, so a redemption run is met in full under the same condition as solvency.

Definition 2.12 (Redemption Run). *A* ***redemption run on*** *p is a maximal finite safe computation of Redeem transactions, each surrendering a p-coin to p and taking a coin of an issuer other than p; it is* ***met in full*** *if $\ell_p = 0$ in its last configuration.*

Proposition 2.13 (Redemption Run). *Every redemption run on p is met in full if $a_p \geq \ell_p$, and otherwise ends with exactly $\ell_p - a_p$ p-coins in circulation, their presentations unfulfilled.*

3 Pen-and-Paper Realisation of Grassroots Currencies

Here we show how people can adopt and follow the contract with paper coins, in a scenario staged in Figure 1 and continued in Section 3.2.

3.1 Grassroots Paper Coins

A person—natural or legal—is identified by their name and signature. Persons include people, communities, cooperatives, corporations, banks, municipalities, and governments. A pen-and-paper grassroots Alice-coin—a *grassroots paper coin*—is written on paper and signed by Alice, in the form of a promissory note, stating the issuer, Alice, and two standing obligations:

1. Alice prices their offerings in Alice-coins and accepts them in payment at these prices; and
2. Alice prices every grassroots coin they hold, of any issuer, at par against Alice-coins.

A grassroots paper coin is thus a signed, transferable undertaking of its issuer, analogous to a promissory note. The obligations written on it are those of an ordinary contract. It promises no sum certain in money, which the bills and notes acts require of a promissory note [3,97], so whether it is one within those acts is a question for each jurisdiction. Alice transfers any grassroots paper coin to Bob by signing it over to Bob and delivering it, so any two persons can transfer any grassroots paper coins between themselves, with no third party; the signatures on the coin record its provenance. We assume that signatures cannot be forged and that signed papers cannot be duplicated ("double-spent"). A coin is a unit, and a holding is a whole number of them; in a practical implementation each Alice-coin has a serial number and is signed by Alice.

The transactions with grassroots paper coins. Alice and Bob swap coins (clause 2) at a meeting, by simultaneous signing-over and delivery, so the swap is physically atomic. A payment and a redemption are Alice's rights under the written obligations: Bob must accept Bob-coins in payment (obligation 1) and must fulfil a presentation of a Bob-coin (obligation 2); declining either is a breach of the coin's terms, actionable at law. A coin redeemed or paid to its

issuer is self-held; whether the issuer keeps or cancels the paper is immaterial, as self-held coins carry no value (Section 2.3).

3.2 A Scenario

Minting and pricing. Figure 1A shows four persons—yellow, blue, green and red—each with a pile of grassroots paper coins they have minted, each pricing their offerings (bananas, apples, tea bags, and a pear) in terms of their own coins. No trade can occur, as no person holds another person's coins.

Mutual credit lines. This is remedied by mutual credit lines, formed by the voluntary swap of grassroots coins among persons who know and trust each other. Each of the four persons seems to trust their immediate neighbours, and therefore in Figure 1B neighbours establish mutual credit lines via coin swaps: four coins swapped between the green and red persons, and three coins between the green and blue and between the blue and yellow persons, resulting in a total of 20 grassroots coins in circulation. Now trade can ensue. For example, the blue person may buy a green tea bag from the green person using the green coin they hold, resulting in Figure 1C.

Arbitrage. In Figure 1C, the green person can buy a banana from the red person for 3 red coins, whereas the blue person can buy a banana from the yellow person for 1 yellow coin (Figure 2D) and then sell it to the green person for 2 blue coins, for a profit of 1 coin, with the green person saving 1 coin (Figure 2E). Arbitrage trading can continue as long as prices differ and there is liquidity between the source and target of the arbitrage trade.

Redemption and chain payment. Having sold the banana to the green person (Figure 2), the blue person wishes to buy the pear of the red person, priced at two red coins, but holds none—only two green coins. They therefore redeem their two green coins from the green person against the two red coins the green person holds (Figure 3F), and pay them to the red person for the pear (Figure 3G). When Alice redeems a Bob-coin from Bob they may take an Alice-coin Bob holds, revoking credit Alice has given Bob; a fresh Bob-coin, to uncover a forgery; or a Carol-coin Bob holds, for a chain payment, for arbitrage, or to reduce their exposure to Bob and increase it to Carol.



Fig. 2. Arbitrage. In Figure 1C, the green person can buy a banana for 3 red coins from the red person, whereas the blue person can buy a banana from the yellow person for 1 yellow coin—an opportunity for arbitrage. **D.** The blue person has bought a banana from the yellow person for 1 yellow coin, and offers it for 2 blue coins. **E.** The green person has bought the banana from the blue person, saving 1 coin and making a 1-coin profit for the blue person.



Fig. 3. Redemption and chain payment. The blue person wishes to buy the pear of the red person, priced at two red coins, but holds none—only two green coins. **F.** The blue person redeems their two green coins from the green person, taking the two red coins the green person holds. **G.** They pay the two red coins to the red person for the pear.

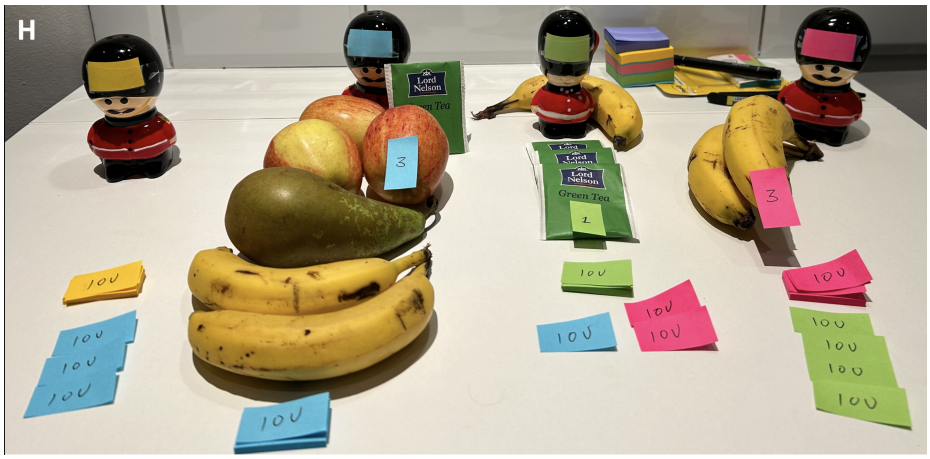


Fig. 4. Insolvency. **H.** After further trades, the blue person holds fruits and a tea bag but no coins of others, while four blue coins remain in circulation: their liabilities exceed their assets, and no presentation of a blue coin can be met with a coin of another issuer—the blue person is insolvent, though they may yet sell their goods to regain liquidity.

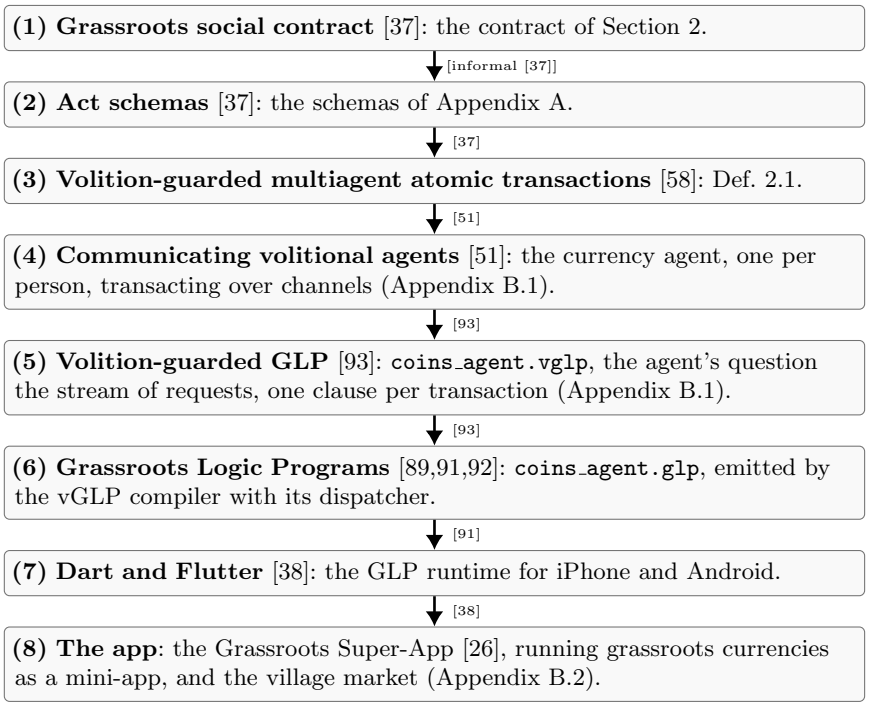


Fig. 5. The abstraction cascade [93] of grassroots currencies, from the contract to the app on each person's phone. Each arrow but the first is an implementation of the abstraction above it by the one below, carrying the reference in which that implementation is defined, and implementations compose [84], so the app implements every abstraction above it; the first arrow is the realisation of the contract, writing its clauses as act schemas, and is the one step left to judgement.

4 Digital Realisation of Grassroots Currencies

In the pen-and-paper realisation of Section 3, people read the contract and follow it on signed notes. Under it, safety and liveness are matters of law and of persons: violating an obligation of the contract is a breach, actionable at law, and so is declining a payment or a presentation (Appendix A.2); and we may assume that whoever persistently wills a permitted transaction with a willing counterparty would eventually perform it. In the digital realisation, both are properties of the program every participant runs [57], and hold of a run in which every party runs it. Here we derive that program from the contract.

4.1 The Abstraction Cascade

The derivation goes down the abstraction cascade [93] of Figure 5, from the contract in natural language (English) to the app on each person's phone, and every artefact of it is in this paper or in `https://github.com/EShapiro2/GLP`. The first two steps are defined in [37]. Each clause that describes an act is written as an *act schema*: who takes part in the act, whose decision it takes, and what each participant must hold, must not hold, gains and loses. Each schema compiles to a *volition-guarded transaction* [58]: a change of the participants' holdings, carried

(1) *Swap*. Alice and Bob, who know each other, may jointly decide to swap coins they hold.

(2) $swap(p?, q?;\ u, k, v, k')$: at p, $knows(q)$, $-k \cdot ¢(u)$, $+k' \cdot ¢(v)$, $+knows(v)$; at q, $knows(p)$, $-k' \cdot ¢(v)$, $+k \cdot ¢(u)$, $+knows(u)$. "Alice and Bob may jointly decide" is the two guarding roles of the swap, and "who know each other" is that each requires *knows* of the other; the mutual credit line is the binding sending u to the party at p, v to the party at q, and k' to k.

(3) $\mathrm{Swap}_{p,q}(¢_u^k, ¢_v^{k'})$, over $\{p, q\}$, guarded by $\{p, q\}$: precondition $q \in K_p$, $p \in K_q$, $¢_u^k \subseteq c_p$ and $¢_v^{k'} \subseteq c_q$; $c'_p = c_p \setminus ¢_u^k \cup ¢_v^{k'}$, $c'_q = c_q \setminus ¢_v^{k'} \cup ¢_u^k$, $K'_p = K_p \cup \{v\}$ and $K'_q = K_q \cup \{u\}$.

(4) The proposal reaches q with the coins given and a response variable, and at q it is the question of a responder, spawned per arriving proposal; the unbound response variable is the pending consent, and binding it commits or aborts the swap: the transaction is taken only when both guards are willing.

(5) The compiler of vGLP prints the platform from the schema and the pragma `Swap: Alice [Swap] <issuer given> <amount given> <issuer wanted> <amount wanted>` and its question line: at p the request `swap(Alice, Bob, u, k, v, k')`, proposed by a tap on `[Swap]` in Bob's row, with the four fields filled; at q the question "Alice asks to swap coins with you.", the binding's values under it by their fields' names, and the answers `yes` and `no`; the transaction is taken only when both have willed it.

(6) The platform compiled to GLP by the canonical compilation, `programs/apps/gc`.

(7) The program runs on the GLP runtime, in Dart, on iPhone and Android.

(8) The Grassroots Super-App runs the mini-app: Bob is asked and answers yes, and each then holds the other's coins (Figure 7); in the village market, Alice and Bob each mint 15 coins and swap them at par.

Fig. 6. The swap, at each layer of the cascade of Figure 5, numbered as there.

out only when every participant whose decision the act takes wills it. Three conditions on the schemas guarantee that the protocol is *volitionally grassroots*: any group of parties can run it on its own, and two groups become connected only by a transaction that a member of each has decided. The schemas of the contract, the modality of each clause—clauses 1–4 are enforced by the contract, clause 5 is undertaken—and the proof that the contract satisfies the three conditions are in Appendix A. The transactions are those of Definition 2.1; the results of this paper are theorems about them, and the transactions of the pen-and-paper realisation are performed on notes, so the results hold under both realisations.

One transaction through the cascade. Figure 6 follows one transaction, the swap by which Alice and Bob open a mutual credit line, from the clause of the contract down the cascade.

4.2 The Protocol

The digital realisation begins by compiling the act schemas to volition-guarded multiagent atomic transactions [37,58], the transactions of Definition 2.1; from these the program every participant runs is derived (Appendix B). A run is *live* if a class of equivalent transactions that is enabled and willed by its guards is eventually taken, and *correct* if it is safe and live; 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 [58]. In a correct run of a protocol, if an equivalence class of transactions is enabled and willed by its guards, then one of its members is eventually taken.

Grassroots. Coins among the members of a group require nothing outside the group, so any group may operate grassroots currencies on its own, and two groups may transact once their members meet and wish to do so.

Corollary 4.1 (Volitionally Grassroots). *Grassroots currencies are volitionally grassroots.*

Proof. The contract is syntactically grassroots (Appendix A), its amounts the values act schemas allow, and the protocol realising a syntactically grassroots contract is volitionally grassroots [37].

4.3 From Volition-Guarded Transactions to a Smartphone App

The app is compiled from the contract. The compiler of vGLP [93] reads the act schemas of Appendix A and the pragmas of the box and prints the platform in vGLP, GLP [89] with volitional procedures: a volitional agent every person runs [51], whose state is the person's holdings and the persons they know, transacting with the agents of other persons over channels, and whose words—the tabs, the buttons, the fields and the questions—are the pragmas'. The platform is compiled to GLP, and the Grassroots Super-App [26] runs it as a mini-app, installing and activating it and rendering its interface; Figure 7 shows four of its screens. The platform and the mini-app are at `https://github.com/EShapiro2/GLP`, in `programs/apps/gc`, and the record of the run of the cascade on the contract in `cascade/GC`. Appendix B.1 derives from the transactions, one by one, a hand-written agent in vGLP, and Appendix B.2 plays a village market of six persons on the app.

The issuer is the sole credit risk. A grassroots coin is its issuer's debt, so trusting the issuer to honour it is unavoidable; we require that the issuer sign every transaction in their own coins, and may not withhold their signature from one the protocol permits, so that holdership of a coin is proven by the issuer's signatures, without trusting the holders it passed through. This is the design of Grassroots Flash [57]; the argument, the treatment of double spending, and the issuer's signed log with its custodian, which we implement, are in Appendix F.

5 Grassroots Economics

This section assumes digital grassroots currencies broadly deployed and used, and presents the economics of the contract in that setting.

5.1 The Contract in Economic Terms

In economic terms, a grassroots coin is an IOU—inside money [14]—issued freely by its issuer, whose offerings and holdings back it. Grassroots currencies rest on one principle: honour thy IOUs. A person endows their coins with value by pricing their offerings in them (clause 5), and the offerings of each person include every coin they hold, of any issuer, priced at par (clause 4). A swap between Alice and Bob in which Alice gives Bob Alice-coins and Bob gives Alice Bob-coins opens a mutual credit line between the two of them.

Set-off and default. Alice redeeming a Bob-coin against an Alice-coin that Bob holds is *set-off*, where each gets their own coin back, at par. An unfulfilled presentation to Alice of an Alice-coin is evidence for Alice's default, which in turn may cause a redemption run on Alice and, if Alice turns out to be insolvent, the depreciation of the market value of Alice-coins.

Backing. The value of a coin rests on what its issuer accepts it for: the issuer undertakes to accept their own coins for their offerings at the prices they post, and to price every coin they hold at par against their own, so the value of a

coin depends on the financial health of its issuer. Coin redemption prices the coins of mutually-liquid persons at par while they meet presentations, hence at equal value. The holder of an Alice-coin who loses trust in Alice may redeem it against any coin held by Alice, or sell it at a discount.

Credit and the sale of debt as coin swaps. Mutual credit, asymmetric credit, and the sale of debt are swaps of grassroots coins (clause 2), each between Alice and Bob and willed by both:

1. **Symmetric mutual credit.** Alice and Bob each mint the same number of coins and swap them. Each thereafter holds that many coins of the other, and trade between them can commence (Figure 1B).
2. **Asymmetric mutual credit.** Alice, with high liquidity, charges a premium for their credit to Bob, a credit-less newcomer, giving fewer Alice-coins than the Bob-coins they receive. The premium is Alice's profit once Bob has liquidity of their own, and Alice's loss if Bob spends the Alice-coins and disappears. As coins are redeemable at par, Alice may redeem the Bob-coins they hold against Alice-coins at once and keep the premium; interest that is earned over time needs a maturity date, which is the subject of grassroots bonds [90].
3. **Sale of debt.** Alice sells Carol-coins to Bob at a discount, receiving fewer Bob-coins than the Carol-coins they give. The debtor Carol is not a party; the discount reflects Alice's doubt about Carol's solvency.

Chain redemption. Redemption reaches across chains of holdings, coin by coin: if each person of a sequence holds a coin of the next, the first can obtain a coin of the last by redeeming along the sequence. Chain redemption enables long-range payments and arbitrage. Consider a group of persons connected by such chains, rational and fully informed about the group. A price difference between two of their coins is an arbitrage: the holder of the low-priced one chain-redeems it for the high-priced one and sells it at a profit, and such chain redemptions continue until the difference is gone or the liquidity along the path is exhausted—low-priced persons disconnecting from high-priced ones by exhausting the liquidity that connects them.

Arbitrage. Mutual liquidity allows arbitrage, staged in Section 3.2: while each person is free to price their offerings as they wish, a price difference for one good combined with liquidity allows arbitrage trading, with intermediaries splitting the profit, so the prices of that good stated in grassroots coins equalise within a liquid economy while the liquidity between the two sides persists, transaction frictions apart.

5.2 Insolvency and Creditworthiness

The issuer may still hand back a coin of their own, which clause 4 permits and which leaves their liabilities where they were. Solvency here is solvency at contractual par: the ratio prices every coin held at one, whatever its issuer's standing, and Appendix D names the assets a lender discounts. Default is sanctioned by the community [6]: holders redeem what the defaulter still holds, no one extends them new credit, they lose set-off and the ability to trade in their own currency, and the market value of their coins depreciates. A solvent person may still lack the coins of a particular issuer; how many they can obtain by their

own redemptions is a maximum flow in the graph of holdings (Proposition 2.11). Figure 4 stages insolvency with paper coins.

Liquidity ratios. The cash, quick, and current ratios of corporate finance stratify the assets by how soon they can be realised; every grassroots coin is redeemable now as of right, so for coins the three coincide in the liquidity ratio; the distinction they draw by asset class is drawn by maturity in grassroots bonds [90]. A worked example on the village market and the dynamics of recovery from insolvency are in Appendix D.

Creditworthiness measures. Determining creditworthiness is an art; still, grassroots currencies offer objective measures for it, analogous to those of international monetary economics: the net external position [47] and velocity [31]. The *net external coin position* of p is $\ell_p - a_p$, the number of p-coins held by others minus the number of coins of other issuers held by p; smaller is better, and its negation is the net investment position of p. The *change in net external coin position* of p over a period is the difference between its values at the end and at the start of the period. The *velocity* of the currency of p is the number of p-coins transferred during a period, divided by the average number of p-coins in circulation during it. A lender assesses a borrower by these measures: a community bank opening credit lines with its members (Section 5.3). The positions sum to zero across the economy, so a member holding a large positive one holds coins others owe.

5.3 The Community Bank

A community bank, or credit union, issues its own grassroots currency and opens credit lines with the members of its community at its discretion, swapping its coins for theirs; its members undertake to accept payments in the community currency, so transactions among liquid members may be one-step payments in it. Such a payment is no transaction of Section 2: clause 3 pays a party coins of their own issue, and here the payee is given coins of the bank. It is an *extension* of the contract, by which a party undertakes to accept named currencies besides their own, and it is what a member's undertaking to the bank adds. Without the extension a member reaches the seller's own currency by chain redemption, at the cost of the coins along the path. The results of Section 2.5 quantify over redemptions, so they hold of a configuration however it arose. The bank needs no external funding to create the initial balances: the personal coins it holds back the community coins it has issued, and it manages its exposure to a member by redeeming that member's coins against coins of others the member holds, without withdrawing credit. Backing is not capital: a bank whose assets equal its liabilities absorbs no loss. The community mutual-credit scenario, the bank's credit lines with its members, the backing, and risk management by redemption are in Appendix E. The bank holds coins of every member and every member holds its coins, so a community's net position is naturally stated against it: whether the members can clear their debts among themselves by redemptions into it, leaving the balance with the bank; how many of the bank's coins a group of members can obtain by their own rights; and whether a run on the bank is met. These are the results of Section 2.5, stated for a designated member—the bank, or any member so designated—the sink.

6 Related Work

The comparisons below are made in full in Appendix H.

Global cryptocurrencies and DeFi. Bitcoin [67] and Ethereum [12,100] keep one replicated ledger by consensus among miners or validators, so a transaction costs computing or locked capital and a fee for its place in the next block; grassroots currencies keep no shared ledger, and a transaction costs the operation of a networked device [57,87]. Smart contracts [12,82,95] carry decentralised finance [79,99]: overcollateralised lending [41,56], automated market makers, and stablecoins. Mutual credit and the sale of debt are swaps of coins (Section 2), and the instruments of grassroots bonds are swaps of bonds and escrow agreements [90], among persons who trust each other and without fees. Flash loans [74], automated market makers, and maximal extractable value [19,73] rest respectively on global atomicity, on pooled shared state, and on a global order of transactions, none of which the grassroots base protocol provides; 181 DeFi attack incidents are systematised in [101].

Payment and state channels. Payment channels [70], state channels [18,24], and other layer-2 designs [40] take transactions off the chain and return to it to settle a dispute; discreet log contracts [23] are bilateral derivatives settled by an oracle's signature; cross-chain atomic swaps [44] exchange assets across two chains; and [9] replaces the chain by a DAG. The abstract grassroots transaction is bilateral and settles with no chain: a party who disowns their signature is in default, remedied at law and made public by the record (Section 5.2).

Credit networks and personal currencies. Mutual credit systems such as LETS keep one unit and one ledger: each member has an account with a central administration, a purchase runs the buyer's balance down or into debt, and the balances sum to zero [80], and the Swiss WIR, since 1934, is a bank keeping such accounts for its members, in credits denominated in but not redeemable for francs [94]; a grassroots coin is the debt of one person to another, in the issuer's own unit, with no administration. Fugger's proposal of money as IOUs in a trust network [34] is an early statement of the idea; the later XRP Ledger [81] realised IOU routing on a ledger with global consensus, and SilentWhispers [60] without a ledger, for payment routing. Ghosh et al. define a trust network, in which a payment is routed as IOUs along links whose capacities are the credit each agent extends the next, and what a set of agents can pay one of them is the maximum flow from the set to it [35]; credit networks [20] route chain payments over bilateral credit lines, and Karlan et al. define network trust as a maximum flow of social collateral [50]; there the edges are capacities to borrow or to route, here they are coins outstanding, and the flow is what a group obtains by redemptions (Proposition 2.11). Sardex [32,48] creates liquidity from trust within a community, with an operator, and Sarafu [61] is one community currency administered by a foundation, its transactions duplicated onto a public blockchain; Holochain's white paper [42] describes a currency as accounting records on the chains of the two parties, each transfer an entry countersigned by spender and receiver, with no global consensus, in a unit the application fixes; Hypersyn [75] is mutual credit with no ledger, consensus or validators, in which each node issues its own credit,

an edge between two nodes holds reserves of both, and a payment moves the reserves by a constant-product rule, so nothing is held, transferred or redeemed; Circles [16,17] mints a personal currency for each account at a fixed rate, with demurrage, swapped one-for-one along a trust graph, and Trustlines [43] hosts mutual-credit networks, both on blockchain infrastructure; FairTrade [46] has each peer of a file-sharing system issue a personal currency, spent by its issuer or by any peer who received it, accepted by its issuer for services and by other peers up to a credit limit each sets the issuer, with no central bank; personal cryptocurrencies were proposed in [77] and sold through an operator by Promify [71]; and Worldcoin [8] is one global currency, at the antipode of a currency per person. Prior work includes mutual credit, personal currencies, payments along paths of trust, routing without a ledger, agent-centric execution, and executable legal contracts. Grassroots currencies are transferable person-issued debts redeemable as of right, specified by a social contract compiled to a program every participant runs, with no shared ledger and no global consensus, and with exact conditions on the holdings for clearing, liquidity and a redemption run.

Clearing in financial networks. Eisenberg and Noe [25] prove that a clearing payment vector, every node paying its creditors pro rata, exists as a fixed point, the basis of the analysis of contagion [36]. Grassroots clearing redeems unit coins in kind at the holder's initiative, and whether a community clears is a comparison of degrees, person by person (Proposition 2.7).

Community finance. Group lending [65]; peer-to-peer lending, where friendship is a credit signal [59] and peers predict default better than credit scores [49]; rotating savings and credit associations [4,7]; and hawala [28] substitute trust within a community for institutional intermediation, as grassroots currencies do; community currencies, reviewed in [64], contribute mostly to social sustainability, their economic benefits limited by their small scale; and 1.4 billion adults have no formal financial services [21]. The creditworthiness measures of Section 5.2 are those of international monetary economics, the net external position [47] and velocity [31]; the scenarios of Appendix E draw on currency areas [66], company scrip [39], and community basic income [5,45].

Bills, notes, and monetary theory. Before banks dominated payment, debts circulated as bills of exchange and promissory notes [76,78]; a grassroots coin is a signed transferable IOU payable on demand, analogous to such a note but promising no sum certain in money, so its status under the bills and notes acts [3,55,97] and what its electronic signature establishes [30,96,98] are questions for each jurisdiction (Appendix F). Grassroots coins are inside money [14,15]; money is memory [52], and here the memory is the record each person keeps; a mutual credit line creates an asset and a liability at once, as bank lending creates deposits [62,68]; and in the framework of [11] grassroots currencies are peer-issued, record-based inside money with neither sovereign backing nor consensus.

Specification and realisation. Financial contracts have been specified declaratively since [69], Marlowe [53] compiles such specifications to consensus-bound smart contracts, Scilla [82] is an intermediate-level smart-contract language, and the Accord Project [1] writes legally binding agreements as text with

machine-executable components, with no blockchain needed; here the currency is specified by a grassroots social contract [37] and realised as a digital social contract [13] that the parties run, on any of the platform classes of [88]; on a grassroots platform a payment involves the payer, the payee and the issuer of the coins paid [57,86]. Self-chosen identities cost nothing [22]; a Sybil's coins are debt with no credit standing behind it, and a graph that friends can see exposes duplicate identities [83]. Enforcement by mutual attestation, intended to leave an attested agent executing correctly or crashing rather than deviating arbitrarily [54], is further work (Appendix F).

7 Conclusion

Grassroots currencies turn mutual trust into liquidity: a coin is its issuer's debt, a mutual credit line is a swap of coins between persons who trust each other, and coin redemption pegs the currencies of mutually-liquid persons at par and carries payments along chains of holdings. The contract of Section 2 states the currency, its four transactions enforced and its pricing undertaking witnessed by every coin in another's hands, and the coins in circulation form a graph on which a redemption acts locally. Whether a community clears, what a group can obtain and whether a redemption run is met are then read from the degrees and the maximum flows of that graph, and need neither coordination among the persons nor a shared ledger. Each person acts by their own rights, and the properties of the whole economy follow from the graph of the holdings those transactions produce.

The contract has two realisations. With pen and paper the obligations are written on the notes, and a breach of them is remedied under the law of the jurisdiction. Digitally they are kept by every correct run of the program derived from the contract schema by schema, and the issuer signing every transaction in their own coins makes the issuer the sole credit risk—the risk already taken when their debt was accepted. Holding a deployment to correct execution needs the assumptions of Appendix F, with mutual attestation left to further work.

A grassroots bond is a debt of its issuer with a date. Its bearer redeems it against coins once that date has come, and it can pay interest, where a coin redeemed at par cannot. Bonds and the financial instruments built on them are the subject of a separate paper [90]. Further work is the economy that is not a demonstration: issuers who default, and populations of thousands rather than six. The secure coins—the issuer's log, its custodians, and recovery from the loss of a signing key or a device—are specified, implemented and proved in [27].

AI Disclosure. The authors used Anthropic's Claude models to assist with two parts of this work. First, the GLP code (Appendix B) was derived from the contract of Section 2 with substantial Claude assistance: the authors specified the contract, supplied GLP language documentation, iteratively reviewed the generated code against the specification and against a running implementation, and made all design decisions. Second, the prose of the paper received Claude assistance for drafting and proofreading under the same review discipline. The authors verified the correctness and originality of all content, including all references. Responsibility for all content rests with the authors.

References

1. Accord Project: FAQ: Accord Project frequently asked questions. https://docs.accordproject.org/docs/accordproject-faq/ (2026), accessed 21 September 2026
2. Agarwal, S., Alok, S., Ghosh, P., Ghosh, S., Piskorski, T., Seru, A.: Banking the unbanked: What do 255 million new bank accounts reveal about financial access? Columbia Business School Research Paper (17-12) (2017)
3. American Law Institute and Uniform Law Commission: Uniform commercial code, article 3: Negotiable instruments (2002)
4. Ardener, S.: The comparative study of rotating credit associations. The Journal of the Royal Anthropological Institute of Great Britain and Ireland **94**(2), 201–229 (1964). https://doi.org/10.2307/2844382
5. Assia, Y., Ross, O.: Good dollar experiment (2021, https://wwwgooddollarorg/wp-content/uploads/2018/11/GD-Wealth-Distribution-Position-Paperpdf)
6. Besley, T., Coate, S.: Group lending, repayment incentives and social collateral. Journal of Development Economics **46**(1), 1–18 (1995)
7. Besley, T., Coate, S., Loury, G.: The economics of rotating savings and credit associations. American Economic Review **83**(4), 792–810 (1993)
8. Blania, A., Altman, S., the Worldcoin team: Worldcoin. https://worldcoin.org (2022)
9. Boyen, X., Carr, C., Haines, T.: Blockchain-free cryptocurrencies: A framework for truly decentralised fast transactions. Cryptology ePrint Archive, Report 2016/871 (2016), also published as "Graphchain" at BCC@AsiaCCS 2018
10. Bruhn, M., Love, I.: The economic impact of banking the unbanked: evidence from mexico. World bank policy research working paper (4981) (2009)
11. 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
12. Buterin, V.: A next-generation smart contract and decentralized application platform. white paper **3**(37) (2014), https://ethereum.org/whitepaper/
13. Cardelli, L., Orgad, L., Shahaf, G., Shapiro, E., Talmon, N.: Digital social contracts: A foundation for an egalitarian and just digital society. In: CEUR Proceedings of the First International Forum on Digital and Democracy. vol. 2781, pp. 51–60. CEUR-WS (2020), https://ceur-ws.org/Vol-2781/paper5.pdf
14. 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)
15. Cavalcanti, R.d.O., Wallace, N.: A model of private bank-note issue. Review of Economic Dynamics **2**(1), 104–136 (1999)
16. Circles: Welcome to Circles: Circles documentation. https://docs.aboutcircles.com/ (2026), accessed 21 September 2026
17. Circles: Circles: A decentralised universal basic income platform based on personal currencies (Retrieved 2021 https://joincirclesnet/)
18. Coleman, J., Horne, L., Xuanji, L.: Counterfactual: Generalized state channels (2018), https://github.com/counterfactual/paper, whitepaper
19. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.: Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 910–927. IEEE (2020). https://doi.org/10.1109/SP40000.2020.00040

20. 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)
21. Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S.: The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. World Bank (2022). https://doi.org/10.1596/978-1-4648-1897-4
22. Douceur, J.R.: The sybil attack. In: Proceedings of the international workshop on peer-to-peer systems. pp. 251–260. Springer, EU (2002)
23. Dryja, T.: Discreet log contracts (2017), https://adiabat.github.io/dlc.pdf, mIT Digital Currency Initiative
24. Dziembowski, S., Eckey, L., Faust, S., Malinowski, D.: General state channel networks. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. pp. 949–966 (2018)
25. Eisenberg, L., Noe, T.H.: Systemic risk in financial systems. Management Science **47**(2), 236–249 (2001)
26. 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
27. 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
28. El Qorchi, M., Maimbo, S.M., Wilson, J.F.: Informal Funds Transfer Systems: An Analysis of the Informal Hawala System. No. 222 in IMF Occasional Paper, International Monetary Fund (2003)
29. Elias, P., Feinstein, A., Shannon, C.E.: A note on the maximum flow through a network. IRE Transactions on Information Theory **2**(4), 117–119 (1956)
30. 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
31. Fisher, I.: The Purchasing Power of Money: Its Determination and Relation to Credit, Interest and Crises. Macmillan, New York (1911)
32. Fleischman, T., Dini, P., Littera, G.: Liquidity-saving through obligation-clearing and mutual credit: An effective monetary innovation for SMEs in times of crisis. Journal of Risk and Financial Management **13**(12), 295 (2020). https://doi.org/10.3390/jrfm13120295
33. Ford, Jr., L.R., Fulkerson, D.R.: Maximal flow through a network. Canadian Journal of Mathematics **8**, 399–404 (1956)
34. 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)
35. Ghosh, A., Mahdian, M., Reeves, D.M., Pennock, D.M., Fugger, R.: Mechanism design on trust networks. In: Internet and Network Economics, Third International Workshop (WINE 2007). Lecture Notes in Computer Science, vol. 4858. Springer (2007)
36. Glasserman, P., Young, H.P.: Contagion in financial networks. Journal of Economic Literature **54**(3), 779–831 (2016)
37. 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)

38. Google: Dart programming language (2024), https://dart.dev/
39. Green, H.: The company town: the industrial Edens and satanic mills that shaped the American economy. ReadHowYouWant. com (2011)
40. Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., Gervais, A.: SoK: Layer-two blockchain protocols. In: Financial Cryptography and Data Security (FC 2020). LNCS, vol. 12059, pp. 201–226. Springer (2020). https://doi.org/10.1007/978-3-030-51280-4_12
41. Gudgeon, L., Werner, S.M., Perez, D., Knottenbelt, W.J.: DeFi protocols for loanable funds: Interest rates, liquidity and market efficiency. In: Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT '20). pp. 92–112. ACM (2020). https://doi.org/10.1145/3419614.3423254
42. Harris-Braun, E., Brock, A., d'Aoust, P.: Holochain: Distributed coordination by scaled consent, not global consensus. White paper v2.0, Holochain Foundation (2024), https://www.holochain.org/documents/holochain-white-paper-2.0.pdf
43. Hees, H., Friis, G., Naerland, K., Howitt, A., Kärki, T., Fletcher, A.: Trustlines network white paper (2021, https://docstrustlinesnetwork/assets/pdf/Trustlines_Network_Whitepaper_2021pdf)
44. Herlihy, M.: Atomic cross-chain swaps. In: Proceedings of the 2018 ACM symposium on principles of distributed computing. pp. 245–254 (2018)
45. Howitt, A.: Roadmap to a government-independent basic income (ubi) digital currency (2019)
46. Hu, Y., Bhuyan, L.N., Feng, M.: Peer-to-peer indirect reciprocity via personal currency. Journal of Parallel and Distributed Computing **72**, 1045–1054 (2012). https://doi.org/10.1016/j.jpdc.2012.04.008
47. International Monetary Fund: Balance of Payments and International Investment Position Manual. International Monetary Fund, Washington, DC, sixth edn. (2009)
48. Iosifidis, G., Charette, Y., Airoldi, 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
49. Iyer, R., Khwaja, A.I., Luttmer, E.F.P., Shue, K.: Screening peers softly: Inferring the quality of small borrowers. Management Science **62**(6), 1554–1577 (2016). https://doi.org/10.1287/mnsc.2015.2181
50. Karlan, D., Mobius, M., Rosenblat, T., Szeidl, A.: Trust and social collateral. The Quarterly Journal of Economics **124**(3), 1307–1361 (2009)
51. Keidar, I., Shapiro, E., friends: Fault-resilient implementations of volition-guarded multiagent atomic transactions (2026), in preparation
52. Kocherlakota, N.R.: Money is memory. Journal of economic theory **81**(2), 232–251 (1998)
53. Lamela Seijas, P., Thompson, S.: Marlowe: Financial contracts on blockchain. In: Leveraging Applications of Formal Methods, Verification and Validation (ISoLA 2018). LNCS, vol. 11247, pp. 356–375. Springer (2018). https://doi.org/10.1007/978-3-030-03427-6_27
54. Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. ACM Transactions on Programming Languages and Systems **4**(3), 382–401 (1982)
55. League of Nations: Convention providing a uniform law for bills of exchange and promissory notes. Geneva, 7 June 1930 (1930)
56. Leshner, R.: Compound governance. Blog post, Compound Labs (2020), https://medium.com/compound-finance/compound-governance-5531f524cf68

57. 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
58. 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
59. Lin, M., Prabhala, N.R., Viswanathan, S.: Judging borrowers by the company they keep: Friendship networks and information asymmetry in online peer-to-peer lending. Management Science **59**(1), 17–35 (2013). https://doi.org/10.1287/mnsc.1120.1560
60. Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M.: SilentWhispers: Enforcing security and privacy in decentralized credit networks. In: Proceedings of the Network and Distributed System Security Symposium (NDSS 2017). Internet Society (2017)
61. 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
62. McLeay, M., Radia, A., Thomas, R.: Money creation in the modern economy. Bank of England Quarterly Bulletin **Q1**, 14–27 (2014)
63. Menger, K.: Zur allgemeinen Kurventheorie. Fundamenta Mathematicae **10**, 96–115 (1927)
64. Michel, A., Hudon, M.: Community currencies and sustainable development: A systematic review. Ecological Economics **116**, 160–171 (2015). https://doi.org/10.1016/j.ecolecon.2015.04.023
65. Morduch, J.: The microfinance promise. Journal of Economic Literature **37**(4), 1569–1614 (1999). https://doi.org/10.1257/jel.37.4.1569
66. Mundell, R.A.: A theory of optimum currency areas. The American economic review **51**(4), 657–665 (1961)
67. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008), https://bitcoin.org/bitcoin.pdf
68. Palley, T.I.: Endogenous money: What it is and why it matters. Metroeconomica **53**(2), 152–180 (2002)
69. Peyton Jones, S., Eber, J.M., Seward, J.: Composing contracts: An adventure in financial engineering (functional pearl). In: Proceedings of the 5th ACM SIGPLAN International Conference on Functional Programming (ICFP '00). pp. 280–292. ACM (2000). https://doi.org/10.1145/351240.351267
70. Poon, J., Dryja, T.: The bitcoin lightning network: Scalable off-chain instant payments. Draft version 0.5.9.2 (2016), https://lightning.network/lightning-network-paper.pdf
71. Promify: Promify white paper. https://promify.io/whitepaper (2022), retrieved 2022
72. Proudhon, P.J., Robinson, J.B.: General idea of the revolution in the nineteenth century. Courier Corporation (2004), original work published 1851
73. Qin, K., Zhou, L., Gervais, A.: Quantifying blockchain extractable value: How dark is the forest? In: 2022 IEEE Symposium on Security and Privacy (SP). pp. 198–214. IEEE (2022). https://doi.org/10.1109/SP46214.2022.9833734
74. Qin, K., Zhou, L., Livshits, B., Gervais, A.: Attacking the DeFi ecosystem with flash loans for fun and profit. In: Financial Cryptography and Data Security – 25th International Conference, FC 2021. pp. 3–32. Springer (2021). https://doi.org/10.1007/978-3-662-64322-8_1

75. Ramabaja, L.: Hypersyn: A peer-to-peer system for mutual credit. arXiv:2206.04049 (2022)
76. Rogers, J.S.: The Early History of the Law of Bills and Notes. Cambridge University Press (1995)
77. de la Rouviere, S.: In the future, everyone will have their own cryptocurrency. https://simondlr.tumblr.com/post/70089813484 (2013), retrieved 2022
78. 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)
79. Schär, F.: Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review **103**(2), 153–174 (2021). https://doi.org/10.20955/r.103.153-74
80. Schraven, J.: Mutual credit systems and the commons problem: Why community currency systems such as LETS need not collapse under opportunistic behaviour. International Journal of Community Currency Research **5**(4) (2001). https://doi.org/10.15133/j.ijccr.2001.002
81. Schwartz, D., Youngs, N., Britto, A.: The ripple protocol consensus algorithm. Ripple Labs White Paper (2014)
82. Sergey, I., Kumar, A., Hobor, A.: Scilla: a smart contract intermediate-level language. In: Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation. pp. 366–381. ACM (2019)
83. Shahaf, G., Shapiro, E., Talmon, N.: Genuine personal identifiers and mutual sureties for sybil-resilient community growth. In: International Conference on Social Informatics. pp. 320–332. Springer, Springer, EU (2020). https://doi.org/10.1007/978-3-030-60975-7_24
84. Shapiro, E.: Multiagent transition systems for composing fault-resilient protocol stacks. arXiv preprint arXiv:2112.13650 (2021), https://arxiv.org/abs/2112.13650
85. Shapiro, E.: Grassroots distributed systems: Concept, examples, implementation and applications (brief announcement). In: 37th International Symposium on Distributed Computing (DISC 2023). (Extended version: arXiv:2301.04391). pp. 47:1–47:7. LIPICS, Italy (2023), https://arxiv.org/abs/2301.04391
86. Shapiro, E.: Grassroots social networking: Serverless, permissionless protocols for twitter/linkedin/whatsapp. In: OASIS '23. Association for Computing Machinery (2023). https://doi.org/10.1145/3599696.3612898
87. Shapiro, E.: A grassroots architecture to supplant global digital platforms by a global digital democracy. arXiv:2404.13468, Proceedings of DAWO'24 (2024), https://arxiv.org/abs/2404.13468
88. Shapiro, E.: Characterising global platforms: Centralised, decentralised, federated, and grassroots. arXiv preprint arXiv:2511.03286 (2025), https://arxiv.org/abs/2511.03286
89. 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
90. Shapiro, E.: Grassroots bonds: Financing by the people, for the people. arXiv:2603.13671 (2026), https://arxiv.org/abs/2603.13671
91. Shapiro, E.: Implementing grassroots logic programs with multiagent transition systems and ai (full version). arXiv:2602.06934. Summary to appear in Proc. of LOPSTR+PPDP'26 (2026), https://arxiv.org/abs/2602.06934
92. Shapiro, E.: Types for grassroots logic programs (full version). arXiv preprint arXiv:2601.17957 (2026), https://arxiv.org/abs/2601.17957

93. Shapiro, E.: Volition elicitation: Operational semantics for people and their machines. arXiv:2607.14138 (2026), https://arxiv.org/abs/2607.14138
94. Stodder, J.: Complementary credit networks and macroeconomic stability: Switzerland's Wirtschaftsring. Journal of Economic Behavior & Organization **72**(1), 79–95 (2009). https://doi.org/10.1016/j.jebo.2009.06.002
95. Szabo, N.: Formalizing and securing relationships on public networks (1997)
96. UNCITRAL: Model law on electronic signatures with guide to enactment (2001)
97. United Kingdom: Bills of exchange act 1882. 45 & 46 Vict. c. 61 (1882)
98. United States Congress: Electronic signatures in global and national commerce act (2000), public Law 106–229, 114 Stat. 464
99. Werner, S.M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., Knottenbelt, W.J.: SoK: Decentralized finance (DeFi). In: Proceedings of the 4th ACM Conference on Advances in Financial Technologies (AFT '22). pp. 446–461. ACM (2022). https://doi.org/10.1145/3558535.3559780
100. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger (2014)
101. Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., Gervais, A.: SoK: Decentralized finance (DeFi) attacks. In: 2023 IEEE Symposium on Security and Privacy (S&P). IEEE (2023). https://doi.org/10.1109/SP46215.2023.10179435

A The Act Schemas of the Contract

This appendix writes the clauses of Section 2 as act schemas [37], states the modality of each clause, and shows the contract syntactically grassroots. The contract extends GKK [37], so it holds GKK's three schemas, cited from there and not restated. Establish adds *identity* at its one role. Meet is guarded in both roles and adds *knows* of the other at each. Introduce is guarded in both roles: the first requires *knows* of the second and of a third person c, and the second gains $knows(c)$. Every role but establish's requires *identity*, which the table below leaves out. Act schemas allow values [37]: an atom's argument may be a number, and an atom added or deleted may carry a multiplicity; a value names no person, so the three conditions and the theorem of [37] concern the persons a schema names and stand as stated. In the repository the schemas are a term the checker of [37] reads, `programs/currencies/coins/GC.glp`, in which $¢(u)$ is $coin(u)$. Compiling a schema [37] determines, at each binding of its variables, a transaction whose participants are the roles and whose guards are the guarding roles, enabled when the roles hold what they require, with effect what they add and delete; two transactions are equivalent if they are one schema at one binding. The four schemas below compile to the transactions of Definition 2.1.

A.1 The Act Schemas

The predicates are GKK's *identity*, of arity zero, and *knows*, of arity one, $knows(u)$ in the state of p saying that p holds u's public key, and one of the contract's own, ¢, of arity one: $¢(u)$ in the state of p is a coin issued by u and held by p. The roles are p and q, Alice and Bob of Section 2; the party variables are u, v and r; the value variables are k and k', for amounts. The four clauses that describe acts become four schemas.

schema	*at its first role*	*at its second role*
$mint(p?;\, k)$:	$+k \cdot ¢(p)$	
$swap(p?, q?;\, u, k, v, k')$:	$knows(q),\ -k \cdot ¢(u),\ +k' \cdot ¢(v),\ +knows(v)$	$knows(p),\ -k' \cdot ¢(v),\ +k \cdot ¢(u),\ +knows(u)$
$pay(p?, q;\, k)$:	$knows(q),\ -k \cdot ¢(q)$	$+k \cdot ¢(q)$
$redeem(p?, q;\, r)$:	$knows(q),\ -¢(q),\ +¢(r),\ +knows(r)$	$-¢(r),\ +¢(q)$

"Alice may decide" is the single guarding role of mint, of pay and of redeem; "Alice and Bob may jointly decide" is the two guarding roles of the swap. "Who know each other" is that each role of the swap requires *knows* of the other, and "whom they know" that pay and redeem require $knows(q)$ at p; and a coin carrying its issuer's public key (Section 2) is that swap and redeem add *knows* of the issuer at the role that receives the coin, while pay adds none, the payee receiving coins of their own issue. The amount minted is the argument k of mint. "Bob-coins they hold" and "a Bob-coin they hold" are that pay and redeem require of p a coin whose argument is q; "any coin held by Bob" is redeem's party variable r, unconstrained. The mutual credit line of clause 2 is the swap at a binding sending u to the party at p, v to the party at q, and k' to k; asymmetric credit is the same binding with $k' < k$, and the sale of debt a binding sending u to a third party (Section 2). A binding at which a role adds what it deletes—the

swap of coins of one issuer for more of the same, or the redemption of a q-coin for a q-coin—determines no transaction [37], which is why the two lots of a swap are of different issuers.

A.2 The Modality of Each Clause

The definitions are [37]'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 is 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 1–4 are enforced. Each permits an act and obliges nothing beyond it, so the runs determine it and every correct run keeps it. Two of them oblige a counterparty, and the schemas above make the obligation self-executing: "Alice may decide" in clause 3 is that pay is guarded by the payer and adds the coins at the payee, and in clause 4 that redeem is guarded by the bearer and deletes the taken coin at the issuer. Neither the payee nor the issuer is asked. No clause of the contract is attested: no act of it carries a warranty, and pay adds a coin naming its issuer and not its payer, so no clause against the payer could be [37]. The modalities of GKK:1 to GKK:3 are stated in [37].

Clause 5 is undertaken. Selling at an advertised price is no 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 swap opening a mutual credit line adds $¢(p)$ in the state of the party at q, naming the issuer p, so the coin in another party's holding is the record of the undertaking. The second obligation written on the paper coin (Section 3.1)—the standing offer at par—is not a further undertaking: its exercise is the redemption act, enforced as clause 4.

A.3 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 who already record each other; the protocol realising a syntactically grassroots contract is volitionally grassroots [37]. The three conditions quantify over the people a state records, and the amounts of the schemas above name no person, so the conditions and the theorem apply to them as stated [37].

Introduction. Meet is an introductory act: it is guarded in both roles, it adds $knows(q)$ at p, naming q, and $knows(p)$ at q, naming p. It is unobstructed: what each role requires, *identity*, is added by establish, a schema of arity one, guarded in its role, requiring nothing and forbidding only the identity it adds, so a person establishes once; and no role of meet forbids anything. It is the introductory act of every contract extending GKK [37].

Provenance. *knows* has traceable provenance: meet adds it naming a role; introduce adds $knows(c)$ at q, where c is an argument of an atom p requires; and swap and redeem add *knows* of an issuer at the receiving role, the issuer being an argument of an atom the other role requires. ¢ has traceable provenance. Mint adds $¢(p)$ at p, naming its own role. Swap adds $¢(v)$ at p and $¢(u)$ at q, and v and u are arguments of the atoms the other role requires. Pay adds $¢(q)$ at q, naming a role. Redeem adds $¢(r)$ at p, where r is an argument of the atom q requires, and $¢(q)$ at q, naming a role.

Volition. Of the schemas of arity two, meet, introduce and swap are guarded in both roles. Pay and redeem are guarded by p, and in each p requires $knows(q)$ and $¢(q)$, atoms of traceable provenance naming q, so the role graph is connected: a party pays or presents a coin only to an issuer they know and whose coin they hold.

The contract is therefore syntactically grassroots, and the protocol realising it is volitionally grassroots (Corollary 4.1, Section 4.2): any group of persons operates grassroots currencies on its own, and two groups become connected only by a meeting willed by both.

B From the Contract to the App

The digital realisation of Section 4 in full: the program every participant runs, derived from the transactions of Definition 2.1 one by one down the cascade of Figure 5, and the village market run on it. The Grassroots Super-App [26] runs the compiled program as a mini-app. Under the digital realisation some of the legal obligations of the coins become self-executing.

Volitions and guards. In the pen-and-paper scenario, a person consents by taking part in the transaction; digitally, standing consents are recorded. The assumption of Section 2.5—that persons act on their rights—becomes the correctness requirement of the framework: in a correct run, a transaction that is enabled and willed by its guards is eventually taken [58]. The protocol so specified is *volitionally grassroots*: two groups become coupled only by a first transaction willed by a member of each (Corollary 4.1).

Three levels, and what this paper establishes of each. The transactions of Definition 2.1 are the abstract acts, each over the two persons the act names, and the results of Sections 2.5 and 4 are theorems about them. The program of this appendix is an executable realisation of those acts among parties who run it, and the village market of Appendix B.2 runs it: what it establishes is that the four transactions compose into a running village market. The countersigned transfer of Appendix F is a third level, in which the issuer signs every transfer of their own coins: a swap in which p and q exchange coins of u and v is one transaction of Definition 2.1, and at the third level it needs the signatures of u and of v besides; a redemption that takes an r-coin needs r's. The third level is the secure coins of [27]: the transactions of Definition 2.1 extended with the issuer's log of every transaction in their coins and with state custodians holding copies of it, the issuer a participant of every such transaction; 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 digital social contract. The contract of Section 2 is realised by the *digital social contract* implementing the currency: the multiagent program that every participant runs, its instances communicating only with each other [13]. Its enforced clauses are kept by every correct run of the program: the issuer withholds no permitted transaction, their own coins are accepted in payment, redemption proceeds against any coin the issuer holds, of the bearer's choice, and the record makes default public (Section 5.2). A party also promises, in its undertaking, to run the certified code; that clause is *undertaken*, its record the undertaking in another party's hands, and it is *enforced* where the hosting platform attests the code [26,37]. Mutual attestation for GLP is further work (Appendix F), so today the enforced clauses of this section rest on the parties running the certified code. The pricing undertaking (clause 5) is performed outside the contract. A person joins an instance of the currency on a friend's invitation, by signing an undertaking to keep the contract towards all its participants and to run its certified code, which the super-app presents to each participant on first contact [26,37]. Enforcement by mutual attestation, default and identity escape, the digital platforms a currency can run on, and privacy are discussed in Appendix F.

Implementation in GLP. Grassroots Logic Programs (GLP) [89] is a multiagent, concurrent, logic programming language running on Dart for smartphone deployment. A grassroots specification is realised as a GLP program, which people load and activate voluntarily on their devices. Here we implement the contract of Section 2 as a program in vGLP [93], GLP with volitional procedures, which put a question to the person: the agent's question is the stream of its person's requests, and it has one clause for each transaction of Definition 2.1 at the party who initiates it. The vGLP compiler compiles it to the GLP program every participant runs, together with the interface constructs it derives from the program; the derivation is in Appendix B.1. The app of Section 4.3 is compiled from the contract by the compiler of vGLP, from the schemas and the pragmas (Figure 7); the agent below is written by hand from the transactions, and the village market of Appendix B.2 runs on it with scripted persons submitting the requests and answering the cards in place of the villagers, and on the compiled app, each villager at their phone (Figure 8).

B.1 From the Transactions to the Program

The program is written in vGLP [93], GLP with volitional procedures: a goal of a volitional procedure puts a question to the person, of the procedure's interactive type, and a clause that reads the person's answer reduces only after the person has given it. The agent is a volitional procedure whose question is the stream of its person's requests, one request for each transaction a party initiates; its one clause asks the question once and passes the stream to `serve`, which has one clause per request, each reading its request at the head of the stream:

```
(Reqs)*agent(Id, UserIn, PeerIn, Convs, Outs, Holdings, Serial) :-
```

```
    serve(Reqs?, Id?, UserIn?, PeerIn?, Convs?, Outs?, Holdings?,
          Serial?).
```

The four transactions of Definition 2.1 are the four requests, one clause each, and the swap has a responder besides, at the counterparty. The program is at `https://github.com/EShapiro2/GLP`: the certified mini-app in `programs/currencies/coins/currency`—its entry `coins(Id, Ui, Convs)`, the source `coins_agent.vglp` and its compilation `coins_agent.glp`—and the types and the village market `village.glp` in `programs/currencies/coins`.

The agent. Each person runs a *currency agent*, the procedure `agent` of the source, whose state is the person's holdings—the atoms $¢(u)$ of Appendix A, each coin as `coin(Issuer, Serial)`—and the serial its next coin takes. Its arguments are its name, its own input, the input from its counterparties, the conversations the social graph hands it, its outputs (the screen and one channel per counterparty), its holdings and its serial; `serve` has the same arguments, with the rest of the stream of requests first. The agent transacts with the agents of other persons over those conversations, and an act arriving from another agent is carried out by the clause that receives it.

Mint. $\text{Mint}_p(k)$ is guarded by p: the request `mint(Amount)`, whose one field is the amount; the effect of its clause is $c'_p = c_p \cup ¢^k_p$:

```
serve([mint(Amount)|Reqs], Id, UserIn, PeerIn, Convs, Outs,
      Holdings, Serial) :-
    ground(Id?), integer(Amount?), Amount? >= 1 |
    create_coins(Id?, Amount?, Serial?, New),
    Serial1 := Serial? + Amount?,
    append_coins(Holdings?, New?, Holdings1),
    show(minted(Amount?), Outs?, Outs1),
    after_change(Reqs?, Id?, UserIn?, PeerIn?, Convs?, Outs1?,
                 Holdings1?, Serial1?).
```

Swap. $\text{Swap}_{p,q}(¢^k_u, ¢^{k'}_v)$ is guarded by p and q. At p it is the request `swap(Friend, GiveCoin, GiveAmount, Wa` the counterparty, the issuer and amount of the coins given, and the issuer and amount of the coins wanted—whose clause tests the precondition $¢^k_u \subseteq c_p$ by selecting the coins given:

```
serve([swap(Friend, GiveCoin, GiveAmount, WantCoin,
            WantAmount)|Reqs], Id, UserIn, PeerIn, Convs, Outs,
      Holdings, Serial) :-
    ground(Id?), ground(Friend?), ground(GiveCoin?),
        integer(GiveAmount?), GiveAmount? >= 1, ground(WantCoin?),
        integer(WantAmount?), WantAmount? >= 1 |
    select_coins(GiveCoin?, GiveAmount?, Holdings?, Status, Give,
                 Rest),
    propose_swap(Status?, Id?, Friend?,
                 lot(GiveCoin?, GiveAmount?),
                 lot(WantCoin?, WantAmount?), Give?, Rest?, Reqs?,
                 UserIn?, PeerIn?, Convs?, Outs?, Serial?).
```

The proposal reaches q with the coins given and a response variable, and at q it is the question of a *responder*, spawned per arriving proposal: a volitional procedure whose question is a card, which its clause writes at once with the offer for the person to see, handing the person the writer of their answer, which `decide_swap` reads with a clause per answer:

```
(card(offer(From?, Want?, Offered?),
      Answer))*respond_swap(offer(From, Want, Offered), Resp?,
      Ans?) :-
    ground(From?), ground(Want?), ground(Offered?) |
    decide_swap(Answer?, From?, Want?, Offered?, Resp, Ans).

decide_swap(yes, From, Want, Offered, Resp?, Ans?) :-
    accept_answer(From?, Want?, Offered?, Resp, Ans).
decide_swap(no, From, _, Offered, Resp?, Ans?) :-
    decline_answer(From?, Offered?, Resp, Ans).
```

The answer `yes` is the person's acceptance and `no` their decline; a proposal the person leaves unanswered stays open, the machine owing nothing to a question its person leaves open [93]. The acceptance reaches q's agent as an input, and the clause receiving it tests the precondition $¢_v^{k'} \subseteq c_q$ by selecting the coins wanted: if they are held it binds the response to them and takes the coins offered, which is the effect $c'_q = c_q \setminus ¢_v^{k'} \cup ¢_u^k$; if not, it declines, returning the coins offered. The response reaches p's agent as an input, and the clause receiving an acceptance takes the coins given, $c'_p = c_p \setminus ¢_u^k \cup ¢_v^{k'}$; a refusal returns p's coins to its holdings. The unbound response variable is the pending consent, and binding it commits or aborts the swap: the transaction is taken only when both guards are willing, as Definition 2.1 states.

Pay. $\mathrm{Pay}_{p,q}(k)$ is guarded by p: the request `pay(Friend, Amount)`, whose two fields are the payee and the amount; its clause tests the precondition $¢_q^k \subseteq c_p$ by selecting the payee's coins:

```
serve([pay(Friend, Amount)|Reqs], Id, UserIn, PeerIn, Convs, Outs,
      Holdings, Serial) :-
    ground(Id?), ground(Friend?), integer(Amount?), Amount? >= 1 |
    select_coins(Friend?, Amount?, Holdings?, Status, Give, Rest),
    do_pay(Status?, Id?, Friend?, Amount?, Give?, Rest?, Reqs?,
           UserIn?, PeerIn?, Convs?, Outs?, Serial?).
```

The coins go to q, whose agent takes them without asking its person—clause 3 is the payer's decision—which is the effect $c'_q = c_q \cup ¢_q^k$. Coins that are not q's own are no payment of clause 3, and q's agent returns them.

Redeem. $\mathrm{Redeem}_{p,q}(r)$ is guarded by p: the request `redeem(Friend, WantCoin)`, whose two fields are the issuer presented to and the issuer of the coin wanted; its clause tests the precondition $¢_q \in c_p$ by taking the coin presented:

```
serve([redeem(Friend, WantCoin)|Reqs], Id, UserIn, PeerIn, Convs,
      Outs, Holdings, Serial) :-
    ground(Id?), ground(Friend?), ground(WantCoin?) |
```

```
take_coin(Friend?, Holdings?, Found, Rest),
do_redeem(Found?, Id?, Friend?, WantCoin?, Rest?, Reqs?,
          UserIn?, PeerIn?, Convs?, Outs?, Serial?).
```

The presented coin reaches q with the issuer wanted and a response variable, and q's agent fulfils the presentation without asking its person—clause 4: it takes the coin back and, if it holds an r-coin, gives it, which is the effect $c'_q = c_q \setminus ¢_r \cup ¢_q$; p's agent, receiving the coin, has $c'_p = c_p \setminus ¢_q \cup ¢_r$. The other half of the precondition, $¢_r \in c_q$, is q's to test, and where it fails the agent refines the act without departing from it: it returns the presented coin with the issuers of the coins it holds, one per issuer, and the bearer chooses among them; a redemption against the disclosed menu is a choice among the redemptions the menu offers, one of which the issuer then takes. The disclosed coins are not locked while the bearer chooses, as locking would leave the issuer waiting on a bearer that never answers.

Conversations. Two agents transact over the root channel of the conversation the super-app opens between their two executions of the program, at an invitation of one friend by the other [26]. The agent takes each conversation from the social graph, adopts its channel, and shows it opened; an act willed towards a party with whom no conversation is open is not sent—the coins stay, and the screen says so. The program has no network entry and no act beyond the four of the contract: the agent transacts only over a conversation the social graph hands it, between two persons who know each other, so the preconditions $q \in K_p$ and $p \in K_q$ of Definition 2.1 hold of every counterparty, and the first act of the contract between them is a swap willed by both, or a payment or presentation by a party who holds the other's coin (Appendix A, Volition).

What the compilation derives. The vGLP compiler [93] produces from the source the GLP program every participant runs, `coins_agent.glp`: the goal of a volitional procedure first sends its question to the *dispatcher*, which spawns a construct process for the question; the construct process has the interface draw the widget of the question's type and binds the question with the person's input, which the dispatcher routes to it. The dispatcher is emitted into the compiled program, so the program needs nothing beyond itself. The app of Figure 7 is compiled from the contract and not from this source: the compiler of vGLP prints the platform from the schemas of Appendix A and the pragmas of Section 2, with the tabs, the buttons, the fields and the questions the pragmas name—the tab Coins listing the coins the person holds, Mint with its amount, and in the row of a person the buttons of the acts that name them, Swap with the issuer and amount given and the issuer and amount wanted, Pay with its amount and Redeem with the issuer wanted; a person asked sees the question and the binding's values by their fields' names, and answers yes or no [93].

B.2 Village Market Demonstration

To demonstrate that the acts of the contract compose into a running village market, we run a village market of six agents on the program: Alice (baker), Bob (farmer), Charlie (carpenter), Diana (doctor), Eve (teacher), and Frank (fisherman). The scenario exercises six operations, each an act of the contract or a swap of Section 2:

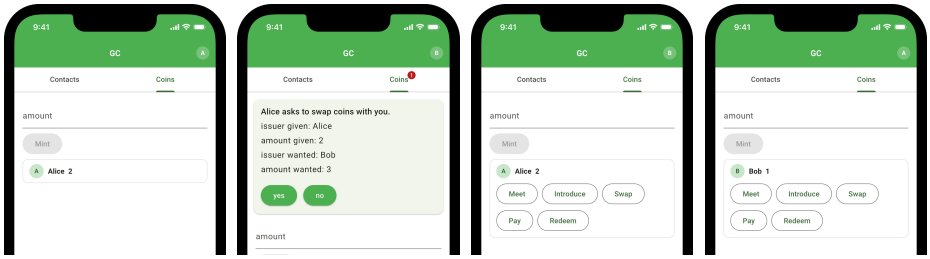


Fig. 7. The GC app. Alice mints two Alice-coins (GC:1); Bob is asked to swap his three Bob-coins for her two Alice-coins, a mutual credit line (GC:2); Bob holds two Alice-coins once he has answered yes, with the buttons of the acts beside them; Alice has paid two Bob-coins to Bob and holds one (GC:3). This is a screenshot of the GC mini-app, compiled from the GC social contract down the abstraction cascade [37,93]. One instance of the app on an iPhone simulator runs the mini-app of every agent; the agents communicate over channels within it, and the screenshot shows one person's screen. All source code and all artefacts, including the social contracts and the artefacts the abstraction cascade produces from them, are in the public repository `https://github.com/EShapiro2/GLP`.

1. **Symmetric mutual credit.** Alice and Bob each mint 15 coins and swap them at par, establishing mutual liquidity. Alice and Charlie do the same with 15 coins each, Charlie and Eve with 10, and Eve and Frank with 10.
2. **Asymmetric mutual credit.** Diana gives Bob 20 diana-coins for 24 bob-coins—a premium of four coins for her credit; Diana similarly gives Frank 15 coins for 18 frank-coins.
3. **Portfolio swap.** Eve trades 5 frank-coins to Charlie for 5 alice-coins, acquiring the currency she needs to buy bread from Alice.
4. **Pay.** Bob pays Alice 5 alice-coins for bread; Eve pays Charlie 6 charlie-coins for a bookshelf; Frank pays Diana 3 diana-coins for a medical checkup; Eve pays Alice 3 alice-coins for bread.
5. **Redeem.** Frank redeems 5 diana-coins from Diana, taking back five of his own coins she holds—set-off, reducing his exposure to Diana's currency.
6. **Sale of debt.** Alice sells 10 bob-coins to Eve for 4 frank-coins—a discounted sale reflecting Alice's desire to reduce exposure to Bob's debt.

The play `village.glp` stands in for the super-app and for the persons: it opens the conversation between every two villagers who transact, seven in all, and hands each villager its conversations on its channel to the social graph, and a scripted person on the other end of each villager's channel to the user interface reads the agent's request form and the cards the dispatcher draws, and the screen the agent writes, and submits its requests and answers the cards in the order of its script, each act once the one before it has taken effect on its screen. The run performs the six operations and ends with the holdings of Table 1. They reconcile with Conservation of Money (Lemma 2.2): every coin is held against its issuer, and the coins of each issuer held across the six agents are the coins they minted—30 alice-coins, 39 bob-coins, 25 charlie-coins, 35 diana-coins, 20 eve-coins and 28 frank-coins—and are those the six operations produce. The

Agent	Holdings after the scenario
Alice	5 bob-coins, 8 alice-coins, 15 charlie-coins, 4 frank-coins
Bob	10 alice-coins, 20 diana-coins
Charlie	10 alice-coins, 10 eve-coins, 6 charlie-coins, 5 frank-coins
Diana	24 bob-coins, 13 frank-coins, 8 diana-coins
Eve	4 charlie-coins, 1 frank-coin, 2 alice-coins, 10 bob-coins
Frank	7 diana-coins, 10 eve-coins, 5 frank-coins

Table 1. The holdings of the six agents at the end of the village market, as each agent's screen reports them, self-held coins included.

same market, played on the compiled app, each villager at their phone and each act a tap, ends with the same holdings: Figure 8 shows the six phones at its end.

B.3 Implementation Summary

The village market of Appendix B.2 is a GLP script that drives the six agents through the six operations. The implementation is open-source: the mini-app is at `https://github.com/EShapiro2/GLP`, in `programs/currencies/coins/currency`, and the village market in `programs/currencies/coins`.

The proof-of-concept represents each coin as a unit. The scenario runs with every party acting as the contract specifies. Three things are left to further work: an issuer who defaults by refusing a presentation they are obliged to fulfil, and the effect on the liquidity ratios of the holders of their coins; concurrent redemptions contending for the same coins, where the menu above is contested; and populations of hundreds of agents, at the scale of the village of Appendix E.

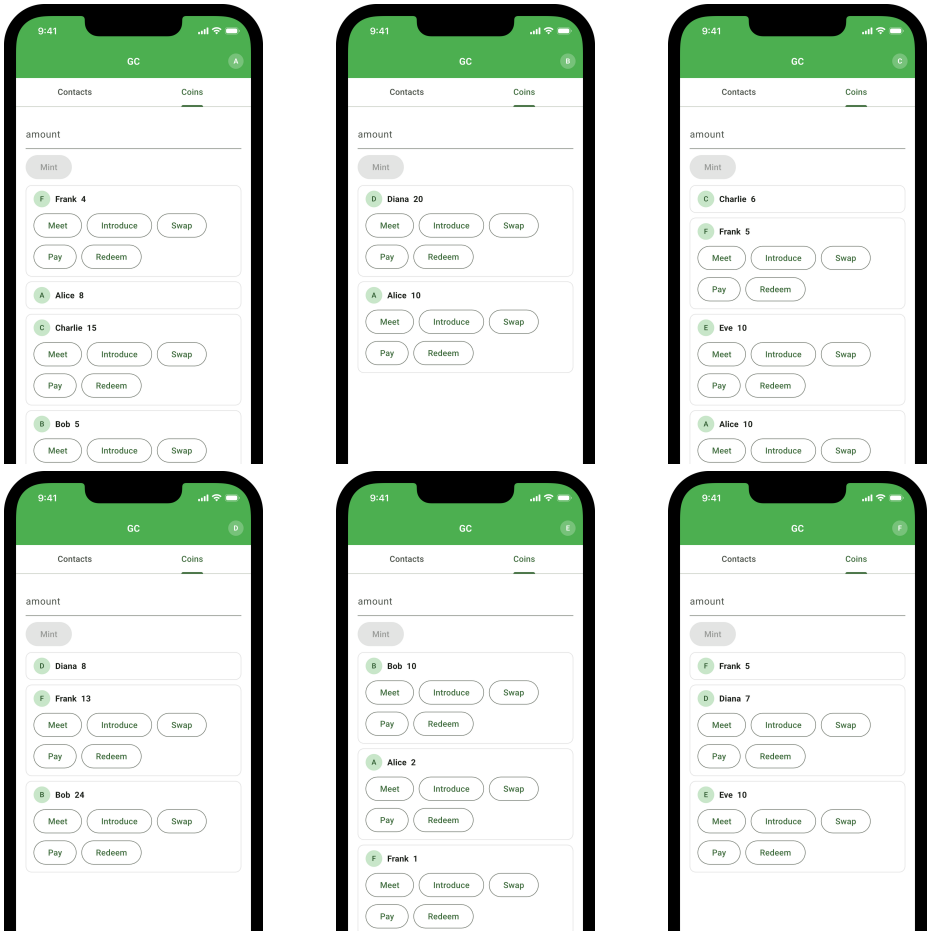


Fig. 8. The six villagers' phones at the end of the village market, Alice, Bob and Charlie above, Diana, Eve and Frank below, each showing the Coins tab of the GC app with the holdings of Table 1. This is a screenshot of the GC mini-app, compiled from the GC social contract down the abstraction cascade [37,93]. One instance of the app on an iPhone simulator runs the mini-app of every agent; the agents communicate over channels within it, and the screenshot shows one person's screen. All source code and all artefacts, including the social contracts and the artefacts the abstraction cascade produces from them, are in the public repository `https://github.com/EShapiro2/GLP`.

C Deferred Proofs

This appendix proves Chain Redemption and the solvency, liquidity, and redemption-run results of Section 2.5. The syntactic conditions establishing that grassroots currencies are volitionally grassroots (Corollary 4.1) are checked in Appendix A.

Proposition 2.4 (Chain Redemption) (restated). *Let $p_0, p_1, \ldots, p_k$ be a sequence of distinct persons with $k \geq 1$ such that each p_i $(0 \leq i < k)$ holds a*

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 a p_k-coin.

Proof. By induction on k. For $k = 1$, p_0 already holds a p_1-coin: zero redemptions suffice. For $k > 1$, by hypothesis p_0 holds a p_1-coin and p_1 holds a p_2-coin, and p_0 knows p_1 (Lemma 2.3). p_0 redeems the p_1-coin they hold against the p_2-coin held by p_1. After this Redeem p_0 holds the p_2-coin, and the sequence $p_0, p_2, \ldots, p_k$ has $k-1$ edges with each of its members holding a coin of the next. By induction, $k-2$ further Redeems put a p_k-coin in the holdings of p_0.

Proposition 2.7 (Graph Solvency) (restated). *The holdings of a sink-closed set V clear into s if and only if $a_p \geq \ell_p$ for every member p of V other than s, and cleared holdings leave each such member holding exactly $a_p - \ell_p$ coins of the sink.*

Proof. A clearing redemption among members of V surrenders a coin of a member $q \neq s$ and takes a coin of q's holdings of an issuer $r \neq q$; if $r \neq s$ then $r \in V$, by sink-closedness of the edge $q \to r$. The surrendered coin becomes self-held and the taken coin moves to the redeemer, so every edge the redemption deletes, creates, or moves is incident to s or has both endpoints in V; edges outside V are untouched, and V remains sink-closed along any safe computation of clearing redemptions among its members.

Write $n_u := a_u - \ell_u$. A Redeem in which holder p surrenders a q-coin and takes a coin y of issuer r held by q changes the counts as follows. The surrendered coin moves to its issuer: a_p and ℓ_q decrease by 1. If $r \notin \{p, q\}$, y moves from holder q to holder p: a_q decreases and a_p increases by 1. If $r = p$, y moves to its issuer: a_q and ℓ_p decrease by 1. If $r = q$, y moves from its issuer to p: a_p and ℓ_q increase by 1. In every case n_u is unchanged for every person u, so every n_u is invariant along any safe computation of Redeem transitions.

Only if: cleared holdings of V have $\ell_p = 0$ for every member p of V other than s, so there $n_p = a_p \geq 0$; n_p is invariant, so $a_p \geq \ell_p$ in the given configuration.

If: by induction on $C := \sum_{p \in V \setminus \{s\}} \ell_p$. If $C = 0$ the holdings of V are cleared. Otherwise some person p holds a coin of an issuer $q \in V \setminus \{p, s\}$, and p is a member of V, as the edge $p \to q$ is incident to s or lies in V. As $a_q \geq \ell_q \geq 1$, q holds a coin y of some issuer $r \neq q$; p knows q (Lemma 2.3), so p redeems the q-coin against y—a clearing redemption among members of V. By the count changes above, the redemption decreases C by 1 or 2 and leaves every n_u unchanged, so the condition persists and the induction applies. At most C redemptions clear the holdings of V.

In cleared holdings of V, every coin of another issuer that a member $p \neq s$ holds is a coin of the sink—its issuer is s or in V by sink-closedness, and every issuer in V other than s is cleared—and there are $a_p - \ell_p$ of them, as n_p is invariant and $\ell_p = 0$ there.

Proposition 2.8 (Clearing Liveness) (restated). *If $a_p \geq \ell_p$ for every member p of V other than s, then every maximal computation of clearing redemptions among members of V ends with the holdings of V cleared into s, after at most $\sum_{p \in V \setminus \{s\}} \ell_p$ redemptions.*

Proof. A clearing redemption among members of V decreases $C = \sum_{p \in V \setminus \{s\}} \ell_p$ by 1 or 2 and leaves every n_u unchanged (proof of Proposition 2.7), so the computation takes at most C redemptions, and $a_p \geq \ell_p$ holds for every member $p \neq s$ in every configuration of it. Suppose the holdings of V are not cleared in the last configuration: some person p holds a coin of an issuer $q \in V \setminus \{p, s\}$, and p is a member of V, as the edge $p \to q$ is incident to s or lies in V. As $a_q \geq \ell_q \geq 1$, q holds a coin y of some issuer $r \neq q$, and p knows q (Lemma 2.3), so the clearing redemption in which p surrenders the q-coin and takes y is enabled there, contradicting maximality.

Proposition 2.11 (Graph Liquidity) (restated). *The liquidity of A is the maximum flow from A to s in G.*

Proof. For the upper bound, for a set S of persons with $A \subseteq S$ and $s \notin S$, let X_S be the number of coins held by a person in S and issued by a person not in S; in the given configuration, X_S is the capacity of the cut at S. A Redeem of a member of A never increases X_S: if the debtor is not in S, the surrendered coin, counted in X_S, moves to its issuer, and the coin taken adds at most one; if the debtor is in S, the surrendered coin is not counted in X_S, and the coin taken, moving from the debtor to the member, is counted after exactly if it was counted before. Every s-coin that a member of A holds in the last configuration is counted in X_S, so their total is at most the capacity of every cut, in particular the minimum, which is the maximum flow.

For the lower bound, take a maximum-size set of pairwise edge-disjoint paths from members of A to s, each simple. Along a path $a = u_0 \to u_1 \to \cdots \to u_m = s$ with $a \in A$ and edge coins $e_1, \ldots, e_m$, a redeems e_1 against e_2, then e_2 against e_3, and so on: its issuer u_i is not a, as the path is simple, a knows u_i, holding e_i (Lemma 2.3), and e_{i+1} is held by u_i, untouched by the preceding redemptions. The $m-1$ redemptions move $e_1, \ldots, e_{m-1}$ to their issuers and e_m to a, and touch no other coin, so the members execute the paths one after another—a path of length 1 being an s-coin its member already holds—and in the last configuration the members of A hold one s-coin per path: maximum-flow many.

Proposition 2.13 (Redemption Run) (restated). *Every redemption run on p is met in full if $a_p \geq \ell_p$, and otherwise ends with exactly $\ell_p - a_p$ p-coins in circulation, their presentations unfulfilled.*

Proof. A redemption of the run surrendering a p-coin to p decreases a_p and ℓ_p by one each: the surrendered coin becomes self-held, and the coin taken, of an issuer other than p, leaves p's holdings. So $n_p = a_p - \ell_p$ is invariant along the run, and the run takes at most $\min(a_p, \ell_p)$ redemptions. Such a redemption is enabled exactly when $\ell_p \geq 1$—some person other than p holds a p-coin, and knows p (Lemma 2.3)—and $a_p \geq 1$—p holds a coin of another issuer. If $n_p \geq 0$ then $a_p \geq \ell_p$ throughout, so a redemption is enabled while $\ell_p \geq 1$, and by maximality the last configuration has $\ell_p = 0$. If $n_p < 0$ then $\ell_p \geq 1$ throughout, so a redemption is enabled while $a_p \geq 1$, and by maximality the last configuration has $a_p = 0$ and hence $\ell_p = -n_p$, the initial $\ell_p - a_p$.

D Liquidity: Worked Example and Recovery

The material deferred from Sections 2.4 and 2.5: assets the ratio counts but a lender discounts, a worked example of the ratio and the measures, the special cases of clearing, the redemption run on one member, and recovery from insolvency.

The liquidity ratio counts assets that may not be realisable: foreign coins that cannot be redeemed, coins of insolvent issuers, and fake assets issued by sybil persons to inflate the balance sheet of p. Grassroots currencies are expected to operate over grassroots social networking [86], where friends reveal their local state to each other, and the local state of a person includes their own neighbourhood: each person sees their friends and their friends' friends. A lender therefore checks the ratio of p against that neighbourhood: whether the issuers whose coins p holds are persons they can see there, or identities with no standing of their own; and whether the holders of p-coins are such persons, or identities of p. Sybil identities cost nothing to create, but a person maintaining mutually-isolated identities in a graph that friends and their friends can see is hard-pressed to do so for long without being exposed [83]; and a mutual credit line is opened only between persons who know each other (Appendix B).

Worked example. We compute the liquidity ratio and the net external coin position of the four persons of Figures 1–4, staged with paper coins. In Figure 1B the green and red persons swapped four coins each, and the green and blue, and the blue and yellow, three each: 20 coins in circulation, every person with a net external coin position of zero and a liquidity ratio of 1. The trades of Figures 1C–4H then move coins as follows: the blue person pays a green coin to the green person (C), a yellow coin to the yellow person (D), and receives two blue coins from the green person (E); redeems their two remaining green coins from the green person against two red coins (F) and pays them to the red person (G); and pays their two remaining yellow coins to the yellow person (H).

At Figure 4H the holdings are: the yellow person holds three blue coins and has none of their own in circulation; the blue person holds no foreign coin and has four blue coins in circulation, three with the yellow person and one with the green; the green person holds one blue coin and two red coins, and has four green coins in circulation, all with the red person; and the red person holds four green coins and has two red coins in circulation, with the green person. Hence, from yellow to red, (a_p, ℓ_p) is $(3, 0)$, $(0, 4)$, $(3, 4)$, $(4, 2)$; the net external coin positions are -3, 4, 1, -2, which sum to zero, as coins are conserved (Lemma 2.2); and the liquidity ratios are undefined for the yellow person, who has no coins in circulation and so no liabilities, 0 for the blue person, 3/4 for the green person, and 2 for the red person. The blue person is insolvent: a redemption run on them leaves all four presentations unfulfilled (Proposition 2.13). The green person, with $a_p < \ell_p$, is insolvent too, by one coin: a run on them is met for three of the four green coins. Since all four started the period with a net external coin position of zero, the changes in their net external coin positions over it are those positions themselves.

Special cases of clearing. Proposition 2.7 has three special cases: (*i*) V is all persons: the economy clears into the sink exactly when $a_p \geq \ell_p$ for every person but the sink—a liquidity ratio of at least 1 where it is defined, and no condition on a person with no coins in circulation—the sink's own coins staying in circulation; it clears completely exactly when every person holds as much as they owe (Corollary 2.9), which by conservation of money is the case of equality throughout. (*ii*) V has no claims on or by the sink: every coin then counts once as an asset and once as a liability within V, so the condition holds only with equality throughout—the community clears exactly when every member holds exactly as much as they owe, and each member ends holding only their own coins. (*iii*) V is a cycle of mutual debt (with the sink an isolated member): the cycle clears with no coins of the sink, as chain redemption around the cycle ends in a set-off. A sink-closed set is the sink together with any union of connected components of the holding graph without it, so one sink serves many communities, each clearing on its own.

The redemption run on one member. For one member, the liquidity ratio reads: the coins they hold cover the coins they owe, and a redemption run is met in full exactly when the ratio is at least 1 (Proposition 2.13). Redemption is the bearer's right under the written obligations and transfers no value, so whether a redemption run is met is a property of the holdings themselves, and an economy all of whose members hold at least as much as they owe clears into any member designated as its sink (Proposition 2.7, case *i*). When $\ell_p > a_p$, the $\ell_p - a_p$ presentations that cannot be met stand unfulfilled, evidencing p's default (Section 2).

Recovery from insolvency. The dynamics of insolvency offers a built-in path to recovery. The longer a person p is insolvent, the less faith—or patience—the holders of p-coins will have for p, and hence they may offer to sell p-coins as bad debt, at an ever-growing discount. The lower the price of p-coins, the easier it is for p to recover: since p prices their goods and services in p-coins, the lower their value, the higher the price p can quote for their goods and services in terms of p-coins and still be competitive. For example, if, following p's insolvency, p-coins trade at a 90%-discount and the market price for mowing a lawn is 11 coins, then p can offer to mow the neighbour's lawn for 100 p-coins and still be competitive. The higher the nominal price of p's goods and services, the faster p can redeem all p-coins in circulation, recover from insolvency, and subsequently regain liquidity, at which point the value of p-coins returns to market value. Those who take a hit in such an insolvency-and-recovery cycle of p are the impatient creditors of p who have sold their p-coins at a discount; those who trusted that p would recover, and bought p-coins at a discount, profit.

E Economic Scenarios

The community bank of Section 5.3 in full, and scenarios beyond it: mutual currency recognition, regional banks, Hawala, private banking, corporation currencies, and a community basic income.

The bank would normally have a governing body and signatories as authorised by the community. Presumably, community members will be happy to use the community currency, knowing that they own the bank.

Community mutual credit scenario. Consider a village with a community of 501 people in which every two villagers swap 100 personal coins with each other. As a result, each villager will have 50,000 coins of other villagers, while issuing and transferring 50,000 of their own coins to others, with 25,050,000 grassroots coins in circulation, solely based on mutual trust among villagers and without any external capital or credit. Such liquidity may jumpstart the village's local economy, with the exposure of each villager to any other initially limited to 0.2% of the total credit they have issued.

Bank–member credit lines. If a community bank is formed and issues 10,000 community coins to each member in exchange for 10,000 personal coins of that member, each member has 50,000 personal coins of others and 10,000 community coins. From that point on the community transacts in community coins, unless a member has exhausted their bank credit and must resort to trading with the personal coins they hold, if any.

Personal credit lines as backing. The p-coins transferred to the community bank are of equal value to the community coins received by p as long as p is liquid; if p becomes insolvent they lose their value. The mutual credit lines between community members and p thus back the community coins the bank has provided to p, though they are unsecured claims and not collateral in the legal sense: the bank holds p-coins, which it may redeem against the coins of other members that p holds.

Bank risk management. Even if the bank initially opens identical credit lines with all community members, it can manage its exposure to members differentially, without withdrawing credit from any of them. If the bank decides that p poses a higher credit risk than other members, for example than members $q_1, \ldots, q_{50}$, it may redeem from p 5,000 of the 10,000 p-coins it holds, in exchange for 100 q_i-coins held by p, for each $i = 1, \ldots, 50$. This decreases the exposure of the bank to p by half and increases its exposure to each of the q_i by one per cent, while leaving p with their 10,000 community coins: the bank reallocates part of its risk with p to creditworthy members who trusted p with a mutual credit line, without harming p's liquidity in community coins. Risk management by redemption is possible only while p is solvent; once it is not, the bank may sell p-coins at a discount (Section 2, sale of debt).

Mutual currency recognition. An alternative to forming a community bank is for community members to mutually recognise each other's currencies: p and q agree to accept each other's coins as payment, each up to a per-issuer limit, as agreed by the parties—the same extension, between two parties rather than a community and its bank. This is a bilateral standing agreement that builds exposure organically as payments flow, without the upfront coin swap of a credit line. If all community members mutually recognise each other's coins, the community forms a currency area without a community bank. Similarly, if two banks

mutually recognise each other's currencies, their customers can transact across banks directly. This mechanism enables bottom-up formation of currency areas.

Regional banks. Several community banks from the same region can cooperate. First, they may establish mutual credit lines, allowing members p, q of different communities a, b to transact via a two-step chain payment: p redeems from their bank a a b-coin, and uses it to pay q. Second, they may form a regional bank c with its own grassroots currency, thus becoming in a sense a single currency area [66]: if the agreement requires members of the communities a and b to accept c-coins, then members of both may transact via c-coins, which they can redeem from their respective banks. Chain redemption ensures an exchange rate at par among personal, community, and regional coins across the region, provided members, communities and the regional bank are mutually liquid. A condition for admitting a new community bank to the regional bank could be sufficient mutual credit lines between the new bank and the member banks, by which the member banks vouch for the good standing of the new one. Such grassroots formation of regional banks may continue to span an entire country, resulting in a country-wide grassroots currency even without the support of the central bank.

Hawala. The thousand-year-old trust-based money transfer system of Hawala [28] can be realised with grassroots currencies. If p wishes to transfer funds to a remote person q, they can do so over the net; but p-coins may be of no use to q if there is no liquidity between p and the merchants in q's locale. A Hawala-like network uses the extension of Section 5.3 instead, in voluntary chain transfers: p transfers locally-liquid coins to their local Hawala agent, and q receives from their local Hawala agent the same number of coins with liquidity in q's locale; credit is settled among the Hawala agents along the path of transfers, as it has been for a thousand years.

Private banking. A member b of the community with initial capital may aim to operate as the community banker, following the footsteps of the Medicis and the Rothschilds. By opening mutual lines of credit with all creditworthy members of the community, the banker's grassroots currency can become the de facto community currency, as all transactions in the community can be completed by a two-step chain payment via the banker: if p wishes to pay q—both with mutual liquidity with the banker b—then p can redeem a b-coin they hold in exchange for a q-coin the banker holds, and then use it to pay q. Naturally, the banker may charge transaction fees. Still, a resourceful community with mutual trust among its members may sidestep the Medicis and the Rothschilds and establish a community bank, owned, operated and governed by the community.

Corporation currencies. In the past, companies with captive employees (e.g., remote mining or logging towns) paid employees in company currency termed scrips, with which the employees could purchase goods at company-owned shops, resulting in the company controlling the entire economy of the town [39]. With grassroots currencies, the situation is the opposite: if a corporation and its employees both use grassroots currencies, then the corporation should pay an employee's salary using the employee's coins. More generally, a corporation, or a

cooperative, may issue its own grassroots currency and price its goods and services in terms of that currency. People who wish to purchase goods and services from the corporation would then have to obtain company currency, via a mutual credit line, by redeeming it from others, or by purchasing it from the corporation at market price. Once customers hold company currency they are captive, and a smart company would do its utmost to keep them and have them purchase as much company currency as possible. A corporation should strive to establish mutual credit lines with its employees, suppliers and customers, providing it with liquidity without external capital or bank credit; such mutual credit lines, if within a given community, could also function as collateral for a mutual credit line between the corporation and the community bank.

Community basic income. A community bank may offer a community-based basic income [5,17,43,45]. To do so, the bank can increase the mutual credit line with members over time, say by one coin a day for each member, even if the member is not creditworthy. The bank thus provides a form of basic income for those who need it, and a kind of basic pension fund for those who do not need additional credit at present. To offset write-offs for members who become insolvent or perish while having a negative net investment position, and to maintain its capital adequacy, the community bank will need contributions from inside or outside the community, in the form of philanthropic donations, government support, or increased income from fees.

F Digital Realisation, Continued

The discussion deferred from Appendix B: the issuer as the sole credit risk, the digital implementations, the legal status of digital coins, enforcement by mutual attestation, default and identity escape, digital platforms, and privacy.

The issuer is the sole credit risk. A grassroots coin is its issuer's debt, so bearing the issuer's credit risk is unavoidable. A paper coin, transferred by the holder signing it over and delivering it (Section 3.1), makes every past holder one too [3,97]. The design reduces credit risk to the issuer; the correctness of the code, the custody of keys, the availability of the issuer and of the custodians, and the certification of the compiler are trust assumptions of their own. For an implementation to add no counterparty beyond the issuer, we require that the issuer p sign every transaction in a p-coin, and that p may not withhold their signature from a transaction that the protocol permits: a payment or redemption of a p-coin by its holder, or a swap the holders of the coins have agreed. Then holdership of a p-coin is proven by p's signatures, and the only counterparty trusted is p, not to disown their signature—the trust already given when accepting p's debt. If p signs conflicting transfers of the same coin (double spending, or equivocation), p's own signatures prove the fraud. On paper, the requirement is met by the issuer countersigning each transfer, naming the new holder: holdership is then proven by the issuer's signature, and nothing more is needed than paper, a pen, and the issuer's signature on each transaction. Note that while p may double-spend a fresh p-coin, this irrational act amounts to economic suicide: it is a signed statement by p that p is not creditworthy, and it results in no financial gain for p, as p could have issued more p-coins instead

of double spending. A recipient doubting a received p-coin may redeem it from p against a fresh p-coin, upon which p either provides such a coin or provides evidence of the double spend.

Digital implementations. The issuer countersigning every transfer of their coins is the design of Grassroots Flash [57], a payment-system protocol for grassroots currencies: a payment in a currency is final when the issuer of the currency approves it, so finality is definite and no consensus is needed. A separate paper [27] makes the loss of a key or machine recoverable: identity and state custodians designated by the person restore both, with the record of their currency recovered exactly and its issuer resuming without double spending. Disowning a key is then a deliberate act, not an accident. We implement this for a currency: the issuer keeps an append-only log of the mints and payments in their own coins, numbered in order; a state custodian reads the log and acknowledges each entry, and the parties take a transaction as final once it is acknowledged. A copy of the log is kept, and the issuer recovers from it the number they resume from. The code is at `https://github.com/EShapiro2/GLP`, in `programs/currencies/secure`, a single-custodian version of the log; the custodian set, finality by a supermajority of custodians, and the recovery of a person's identity and holdings are specified, implemented and proved in [27]. The decisions behind the code are in Appendix G.

Digital coins. A grassroots coin can be implemented as a cryptographically-signed digital IOU: the issuer's identity is 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 [98]; 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 [30]; and the UNCITRAL-model acts say the same where they are adopted [96]. Electronic form therefore presents no obstacle of the kinds these statutes address, and the ordinary rules of contract formation and enforceability remain applicable: a digital grassroots coin is a signed, transferable IOU of its issuer. Three propositions are distinct and only the first follows from the statutes above: that the record is admissible and not denied effect for being electronic; that the obligation it states is an enforceable debt, which depends on the ordinary rules and on the jurisdiction; and that the instrument is a negotiable note within the bills and notes acts [3,55,97], which it does not claim, a grassroots coin promising no sum certain in money. The protocol records the provenance of each coin and prevents its double spending [57], serving the purpose that transfer and proof-of-holdership rules serve for paper notes; the record serves that purpose whatever status a jurisdiction grants it. Identities are self-chosen keypairs, so fictitious issuers—Sybil identities [22]—cost nothing to create. Such an identity issues debt with no credit standing of its own; which legal person the debt is attributable to, and whether issuing it was fraudulent, depend on the facts and on the applicable law. Grassroots currencies are thus cryptocurrencies, resting on the same cryptographic foundations as the global ones; the substantive dis-

tinction is between *global* cryptocurrencies—Bitcoin, Ethereum—and *grassroots* cryptocurrencies (Appendix H).

Enforcement by mutual attestation. A digital social contract is a voluntary agreement—but once adopted, participants must not be able to deviate from the contract as programmed. Smart contracts achieve this through global consensus among third-party validators on a blockchain; the grassroots currencies transactions involve only bilateral interactions, with no need for global agreement on the order of events, so safety reduces to ensuring that each participant is running the correct code, while liveness needs the agents a transaction names to be available besides. This can be achieved by mutual attestation: when two agents communicate, each proves to the other that the message was produced by a correct execution of the agreed-upon contract module. The threat model intended is that an attested agent either executes correctly or crashes, rather than deviating arbitrarily [54]. The contract runs on the participants' own devices, and compliance is verified bilaterally. Realising mutual attestation for GLP, and establishing that model of it, are left to further work. Until it is realised, a party who runs other code is in breach of their undertaking (Appendix B) and is not prevented by the platform.

Default, disappearance, and identity escape. As in real life, indebted people can default, disappear, or change identity. An insolvent person may opt to escape their obligations by abandoning their digital identity and starting afresh—not unlike bankruptcy, but unregulated. Bankruptcy is a regulated process that aims to mitigate the damage to creditors, whereas shedding one's digital identity and assuming another is akin to fleeing the country in order to escape creditors. To avert that, a mechanism to deal with duplicate identities (Sybils) of the same person is needed [83]: if the holder of p-coins discovers that p and p' are identities of the same person, then they may rightfully try to redeem their p-coins from p'. Any individual faces death, after which they cannot consume or produce; the net investment position of a person upon death determines whether the holders of their coins can redeem them or suffer a loss. We leave open the question of inheritance and the management of the estate of a grassroots currency account, noting that accounts held by several signatories are suited to any method devised to address it.

Community-level risk management (Section 5.3), and the collateral and escrow of grassroots bonds [90], provide measures to mitigate such risks, just as their traditional counterparts do. In a grassroots digital economy, mutual credit lines serve a dual role: they provide liquidity, and they back the credit community banks extend. The credit granted to a community member by their peers offers the best mechanism of sybil-resilience, since mutual credit lines are established between people who know and trust each other, making the risk of a correct person opening a mutual credit line with a fake identity low.

Digital platforms. Digital IOUs can be realised on any of the existing digital platforms [88]: centralised, with an operator such as a bank or the sovereign storing the record; decentralised, with smart contracts on a blockchain storing it; federated, with community and institution servers storing it for their members;

and grassroots, with no global infrastructure and no third party between any two agents—each person storing their own record [57].

On a grassroots platform, a payment involves no one but the payer, the recipient, and the issuer of the coins paid—the recipient and the issuer being one party under clause 3, and two under the extension of Section 5.3: the three can transact whenever they can communicate—offline included—instantly and at no cost, regardless of the state of everyone else. Offline covers physical proximity and local networks: nearby phones can communicate directly over Bluetooth, and phones on the same local network can communicate over it even when the network is disconnected from the wider Internet. The other classes place a third party inside every payment—the operator, the consensus nodes and their fees, the parties' servers—so each payment bears that party's availability and cost.

Privacy. A payment employs the public keys of its parties, so it can be encrypted and known only to them. The provenance of a coin must be visible for the payee to check its integrity, and all transactions in p-coins eventually become visible to p, who countersigns them. Still, privacy from p can be maintained by anonymous sub-accounts: a person q who issues a currency must have their public key known to their social and economic circle, but may maintain an additional anonymous identity q' that does not issue a currency, used by q to send and receive payments indirectly. Privacy veils may have to be lowered among persons who offer each other mutual credit lines, as each should be aware of the financial state of the other—in line with common business practice, and with grassroots social networking, upon which grassroots currencies are expected to operate: friends reveal their local state to each other [57,86].

G Implementation Notes

The decisions behind the secure-currency code of Appendix B, at `https://github.com/EShapiro2/GLP`, in `programs/currencies/secure`. Two things they depend on. GLP admits one writer and one reader occurrence of a variable, and a reader occurrence in a guard does not count [89]. And each entry of the issuer's log carries, besides its transaction, references to the acknowledgements the issuer has seen—its *tips*—so the log and the acknowledgements are interlaced.

1. *The first entry carries no tips.* The issuer's tips are the custodian's acknowledgements and the custodian's acknowledgements are of the issuer's entries, so the first entry is produced by a procedure of its own, with no tips, and the loop starts from the second.
2. *The acknowledgement stream is split rather than read twice.* It has two readers—the collection of tips, which feeds them back to the issuer, and the binding of finality—so it is split in two, under the relaxation that admits two reader occurrences of a ground value.
3. *A payment carries one reply variable per party.* The payer and the payee each get an unbound variable the issuer binds, rather than sharing one, so each has a single writer and a single reader.
4. *Finality is bound from a parallel stream read in step with the acknowledgements.* The reply variables are taken out of the approval requests into a stream

of pending entries, and bound when the acknowledgement of the matching number arrives; both streams are in entry order, so they stay aligned.
5. *Tips are collected without waiting.* The acknowledgement stream is read on the test for an unbound tail: an acknowledgement that has arrived is taken as a tip, one already taken is skipped, and an empty stream yields none. Producing an entry therefore never waits on the custodian.
6. *Recovery is a second entry point, not a change to the first.* The wiring that keeps a copy of the log is separate, so the run without recovery is untouched by it.
7. *The copy of the log is taken from the issuer's own stream.* The custodian consumes entries and emits acknowledgements, and returns no copy; the copy stands for what a custodian would hold.
8. *The number is recovered from a closed stream.* The copy closes when the issuer runs out of requests, and walking it then yields the number of the last entry, or zero for an empty log.
9. *Recovery relies on the log only growing.* Any copy of it is a prefix, so the number it ends at is one the issuer may resume from.
10. *The recovered number is compared in a guard.* A reader occurrence in a guard does not count, so the comparison leaves the single-reader rule intact.
11. *Tips are collected from a list of acknowledgement streams.* There is one custodian, and a second is a longer list rather than a change to the collection.

H Related Work, Continued

The comparisons of Section 6, in full.

H.1 Global Cryptocurrencies

Global cryptocurrencies such as Bitcoin [67] and Ethereum [12] are unbacked digital assets whose scarcity and transaction cost are controlled by the protocol. Grassroots currencies differ from global cryptocurrencies in their foundations, architecture, and the financial instruments they support. This section develops these contrasts along four axes: architectural design, source of value and liquidity, the nature of the financial instruments each system supports, and the attacks each design is open to.

Architecture. Global cryptocurrencies maintain a single replicated ledger—a totally-ordered blockchain—via consensus among miners or validators. This architecture entails well-known costs: proof-of-work entails high-cost computing [67]; proof-of-stake requires capital lockup [100]; and a validating node maintains a copy of the global state. Transaction throughput is bounded by block size and block interval, and transaction fees arise from competition for inclusion in the next block.

Grassroots currencies employ a different architecture. Transaction cost is limited to operating a networked device. The system is grassroots [87]: multiple independent deployments can emerge without global resources and interoperate once interconnected.

The comparison table in [57] details 18 dimensions along which the two architectures differ, including: one cryptocurrency per blockchain vs. one per person,

mutually pegged; competitive block creation vs. decentralised and cooperative; global all-to-all dissemination vs. local grassroots dissemination; probabilistic finality vs. definite finality; and a business model based on ICOs and miner remuneration vs. a public good.

Source of value and liquidity. Bitcoin and Ether derive their value from market demand; they are unbacked, and liquidity is obtained by mining or purchasing with external capital. Fiat-backed stablecoins are a class apart, backed by reserves. Grassroots currencies are closer to 'inside money' [14]—a medium of exchange backed by private credit. Each person backs their coins with their offerings: goods and services for people and corporations; interest and transaction fees for banks; taxes for municipalities; and fiat currencies for central banks. Liquidity arises not from capital injection but from mutual credit lines among persons who trust each other, and coin redemption—the obligation to redeem any coin one has issued against any coin one holds—pegs mutually-liquid currencies at par. Grassroots bonds [90] extend this foundation with interest-bearing credit.

Financial instruments on blockchains. The programmability of blockchains via smart contracts [12,82,95] has given rise to Decentralised Finance (DeFi) [79, 99], which re-implements traditional financial instruments on-chain. Lending protocols [41,56] offer overcollateralised loans with algorithmically-determined interest rates; decentralised exchanges provide token trading via automated market makers; and stablecoins offer price-stable media of exchange.

Mutual credit and the sale of debt are voluntary swaps of grassroots coins (Section 2), without a blockchain or consensus, and the instruments built on grassroots bonds—loans, credit lines, options—are voluntary swaps of bonds and escrow agreements [90]. Two differences are noteworthy. First, many permissionless DeFi lending protocols use overcollateralisation enforced by smart contracts, counterparty identity being pseudonymous and trust absent; grassroots credit is extended among persons with mutual trust, and collateral is available but not mandatory. Second, DeFi instruments incur gas fees for every state transition; grassroots transactions incur no fees beyond bilateral communication.

Crypto-native constructs. Three constructs of the blockchain architecture rest on properties grassroots currencies do not have—a globally shared, ordered and atomic state—so the attack surfaces characteristic of them do not arise from the base protocol here: flash loans, automated market makers (AMMs), and maximal extractable value (MEV). A comprehensive systematisation analyses 181 real-world DeFi attack incidents [101].

Flash loans [74] are uncollateralised loans that exist within a single atomic blockchain transaction: a borrower takes a loan, uses the funds across arbitrarily many smart contracts, and repays within the same transaction; if repayment fails, the entire transaction reverts. This is possible because blockchain transactions are atomic across the global state. Grassroots currencies have no global atomic transaction spanning many parties, so a loan taken and repaid within one such transaction has no counterpart in the base protocol. Flash loans are a major

attack vector against DeFi protocols, with documented exploits yielding returns exceeding 500,000% [74]; the base protocol offers no such transaction to exploit.

AMMs provide algorithmic price discovery via pooled liquidity and a bonding curve (e.g., the constant product formula $x \cdot y = k$). On a blockchain the liquidity pool is globally-shared state maintained by consensus. Grassroots currencies have no pooled global state in the base protocol; price discovery is by bilateral negotiation. The trade-off is that grassroots currencies lack automated price discovery but have no pool, so neither impermanent loss, the exposure of a liquidity provider, nor the concentration of value in pool contracts that creates targets for exploitation, and no transaction order for sandwich attacks [19].

MEV [19] is the value extracted through control of the inclusion, exclusion and ordering of transactions in a block. MEV manifests as frontrunning, backrunning, and sandwich attacks, and has been estimated to extract hundreds of millions of dollars annually from Ethereum users [73]. MEV is an artefact of a block producer ordering a global sequence of transactions. Grassroots currencies have no global ordering and no block producer—each person's record is their own—so extraction by ordering does not arise in the base protocol.

Summary. Grassroots currencies occupy a different point in the design space than global cryptocurrencies and their DeFi instruments. Where global cryptocurrencies operate among strangers through consensus at the cost of high transaction fees, capital requirements, and exposure to flash-loan attacks, MEV extraction, and sandwich attacks, grassroots currencies operate without consensus through bilateral trust at the cost of requiring social relationships for liquidity. The financial instruments built on grassroots bonds are comparable in expressiveness [90], but differ in their trust assumptions, cost structure, and the attacks they are open to.

H.2 Finance

Here we survey additional related work: trust-based lending, informal community finance, financial contract specification, credit networks, IOU-based currencies, mutual credit systems, promissory notes, off-chain payment protocols, and monetary theory.

Microfinance and peer-to-peer lending. The Grameen Bank model demonstrated that trust-based, collateral-free lending can work at scale via group liability [65]. Online peer-to-peer lending platforms extended this principle digitally: Lin et al. [59] showed that friendship networks on Prosper.com function as credible credit signals, increasing funding probability and predicting lower default rates; Iyer et al. [49] found that peer lenders predict defaults 45% more accurately than credit scores. Grassroots currencies formalise this trust infrastructure: where microfinance relies on group liability and P2P platforms on centralised matching, grassroots currencies encode bilateral trust directly as mutual credit lines, with creditworthiness assessable via the measures of Section 5.2. This is relevant to financial inclusion: the World Bank Global Findex [21] estimates that 1.4 billion adults worldwide lack access to formal financial services, often in communities where mutual trust is abundant but capital is scarce—the conditions under which grassroots currencies can bootstrap a local digital economy.

Informal community finance. Rotating savings and credit associations (ROSCAs)—known as chit funds, tontines, or *susus* across cultures—are the dominant informal financial instrument in developing economies. Besley et al. [7] proved formally that both random and bidding ROSCAs yield higher utility than autarky by enabling earlier access to indivisible goods through community-based mutual commitment, without formal institutions. Ardener [4] provided the foundational cross-cultural survey documenting their global prevalence. Hawala networks [28] transfer value across borders on pure trust, without formal banking infrastructure. All three—ROSCAs, hawala, and grassroots currencies—share the same foundation: bilateral trust within a community substitutes for institutional intermediation. Grassroots currencies can be viewed as a digital formalisation of the same principle, and grassroots bonds [90] extend it with the expressiveness of a bond market.

Financial contract specification. The foundational work on composable financial contract specification predates blockchain: Peyton Jones et al. [69] introduced a combinator library for describing financial contracts declaratively, inspiring subsequent blockchain domain-specific languages. Marlowe [53], Cardano's financial contract DSL, specifies instruments declaratively with exhaustive static analysis, for execution on a blockchain; Scilla [82] is an intermediate-level smart-contract language, automata-based, for verified contracts on a blockchain. Both run under blockchain consensus. The Accord Project [1] writes a legally binding agreement as natural-language text with machine-executable components—a template, a data model and logic—and is blockchain-agnostic, a blockchain not being necessary; its clauses execute against external systems, where a grassroots social contract is compiled to a protocol its parties run. Grassroots currencies take the same declarative approach—the currency is specified by a grassroots social contract (Section 2), and every transaction is an act of it—but enforce it by the participants' execution rather than via consensus, with each issuer guaranteeing the security of transactions in their currency [57]. To the best of our knowledge, no prior work specifies a currency by a social contract in natural language, derives from it the transactions of a multiagent protocol, and realises them by a program its participants run with no global execution layer.

Credit networks. Credit networks [20] study liquidity in networks of bilateral credit lines, with chain payments as the key instrument. Grassroots currencies inherit this structure: mutual credit lines formed via coin swaps, together with coin redemption, provide for chain payments as in credit networks. Much of the body of knowledge regarding liquidity in credit networks carries over to grassroots currencies, with the caveat that lack of liquidity not only causes chain payment failures but also devalues the currencies of the liquidity-constrained parties involved.

Clearing in financial networks. Eisenberg and Noe [25] model an economy of interbank obligations and prove that a clearing payment vector—every node paying its creditors pro rata out of what it holds and receives—exists as a fixed point; the model grounds the analysis of contagion and systemic risk in financial networks [36]. Grassroots clearing differs: obligations are unit coins, redeemed in

kind at the holder's initiative rather than paid pro rata in a common numéraire; whether a community clears is a comparison of counts, person by person (Proposition 2.7), with the sink's coins the residual holding; and what a group of holders can realise now is bounded by a maximum flow (Proposition 2.11).

Liquidity as network flow. Ghosh, Mahdian, Reeves, Pennock and Fugger define a trust network as a decentralised payment infrastructure in which payments are routed as IOUs between trusted entities, over directed links whose capacities are the credit one agent extends another; what a set of agents can pay one of them is the maximum flow from the set to it, a budget constraint on the set [35]. Karlan, Mobius, Rosenblat, and Szeidl define network-based trust as the largest amount one agent can borrow from another, a maximum flow of social collateral over trust links [50]; in credit networks, a payment goes through exactly when the maximum credit flow from payer to payee covers it, the model behind Ripple-style path-based settlement [20]. In all three, the edges are capacities—permissions to borrow or to route—and the question is point-to-point feasibility. Here the edges are coins already outstanding, the sink is the designated member, and the maximum flow is the number of their coins a group can obtain by redemptions (Proposition 2.11).

IOU credit networks and personal currencies. Fugger's proposal that money can be represented as IOUs in social trust networks [34] is an early articulation of the idea underlying grassroots currencies. The later XRP Ledger [81] put IOU routing on a ledger with global consensus. SilentWhispers [60] proposed a distributed, privacy-preserving credit network that requires no ledger, but it addresses only payment routing, not the richer financial instruments that grassroots bonds support. Holochain [42] is an agent-centric framework with no global consensus: each agent keeps its own hash chain, and its white paper describes a currency as accounting records on the chains of the parties, a transfer is one entry countersigned by spender and receiver, and a double spend is a fork of the spender's chain, exposed by the application's shared database or remedied socially. A grassroots coin is its issuer's debt in the issuer's own unit, transferable and redeemable as of right, and its issuer countersigns every transfer of it. Hypersyn [75] is a peer-to-peer mutual credit protocol with no consensus algorithm, no distributed ledger and no validators: each node creates its own credit, an edge between two nodes holds reserves of both credits, a payment adds the payer's credit to the edge and removes the payee's by a constant-product rule, so the exchange value of a node's credit is set by the reserves on its edges and updated by arbitrage around triangles of nodes; a node cannot hold another node's credit, so nothing is transferred and nothing is redeemed. A grassroots coin is held, transferred and redeemed, and priced at par by its issuer's undertaking. Grassroots currencies implement Fugger's vision without blockchain: personal coins are IOUs traded via bilateral transactions, with coin redemption pegging mutually-liquid currencies at par. Grassroots bonds extend this by adding maturity dates, enabling interest-bearing credit.

Mutual credit and community currencies. Mutual credit systems are the closest precedent to grassroots currencies' approach. LETS, the most widely

implemented, are pure accounting systems of exchange: each member has an account with a central administration unit recording transfers in units, a member creates money by going into debt, and all accounts sum to zero; their stability rests on credit limits, monitoring and sanctions against over-issue [80]. Grassroots currencies have no common unit and no administration: a coin is the debt of its issuer to its holder, in the issuer's own unit, and the issuer backs it. The Swiss WIR, founded in 1934, is the largest and oldest exchange based on a private form of money: a bank keeping an account for each member firm or household in credits denominated in, but not redeemable for, Swiss francs, with a limit on the negative balance; its turnover rises when ordinary money is short, so it is counter-cyclical [94]. A systematic review of community currencies finds that they contribute mostly to social sustainability, their economic benefits limited by their small scale [64]. Sardex, a mutual credit network in Sardinia, achieves significant real-economy impact; its cyclic transaction structure has been analysed in *Nature Human Behaviour* [48]. The Sarafu community currency in Kenya [61], one currency administered by a foundation with its transactions duplicated onto a public blockchain, is an academically-studied digital community currency deployment. Sardex creates liquidity from trust within a community without external capital—the same principle underlying grassroots currencies—but relies on a centralised operator, and a member's debt or credit is not bilateral towards another member but towards the circuit as a whole, on a credit line the circuit manager sets [32]; Sarafu relies on its administering foundation. A grassroots coin is the debt of one person to another.

Circles [16,17] implements blockchain-based personal currencies: every account mints its own at a fixed rate, with demurrage, and the currencies are swapped one-for-one along the social trust graph, so a payment reaches a stranger through a path of trust. Its trust relation authorises the exchange; a grassroots holding is a debt already extended, on which redemption acts. The Trustlines Network [43] implements mutual-credit networks on blockchain infrastructure, with bilateral credit lines similar to those of grassroots currencies but under blockchain consensus.

Personal currencies. FairTrade [46] is an incentive scheme for peer-to-peer file sharing in which each peer issues a personal currency, spent by its issuer or by any peer who received it; the issuer must accept its own currency as payment for its services, which is what gives it value, and every other peer accepts it up to a credit limit it sets the issuer by the issuer's trading history, with no central bank or authority. Its currencies are claims on the issuer's services, and a holder has no right to redeem one against what the issuer holds. The idea of a personal cryptocurrency was floated around a decade ago [77]. Promify [71] enabled artists and celebrities to issue their personal coins and sell their fans exclusive or preferred access to content or merchandise in exchange for these coins—a proof of the viability of personal currencies, yet controlled by a third party. Worldcoin [8], which aims to offer a single global currency for the multitudes, lies at the antipode of grassroots currencies: it is one global currency, where grassroots currencies are one per person. Prior work includes mutual credit, personal cur-

rencies, payments along paths of trust, routing without a ledger, agent-centric execution, and executable legal contracts. Grassroots currencies are transferable person-issued debts redeemable as of right, specified by a social contract compiled to a program every participant runs, with no shared ledger and no global consensus, and with exact conditions on the holdings for clearing, liquidity and a redemption run.

Bills of exchange and promissory notes. Before banks dominated payment, debts circulated as bills of exchange and promissory notes—signed promises to pay—traded and discounted [76,78]. A grassroots coin is analogous to such an instrument, in digital form: a signed, transferable debt payable on demand, sold at a discount (sale of debt, Section 2), with the protocol serving the purpose that transfer and proof-of-holdership rules serve for paper notes (Appendix B); and each coin is the debt of its issuer: past holders bear no liability for it.

Payment and state channels. Layer-2 scaling solutions reduce but do not eliminate reliance on blockchain consensus [40]. Payment channels such as the Lightning Network [70] enable off-chain bilateral transactions but fall back to the blockchain for dispute resolution. State channels [24] generalise this to arbitrary state transitions. Boyen et al. [9] proposed blockchain-free cryptocurrencies using a DAG structure, a prior attempt at the same design goal as grassroots currencies. The abstract transactions of grassroots currencies are bilateral and resemble state channel updates in structure, but differ: state channels derive their security from the ability to publish the latest state on-chain in case of dispute, while grassroots currencies derive theirs from the participants' execution and the issuer's countersignature, with no blockchain fallback. The voluntary swap of grassroots coins is related to cross-chain atomic swaps [44], which exchange assets across two blockchains with no trusted third party; grassroots currencies achieve the same atomicity between the two parties, without any blockchain. Discreet Log Contracts [23] are bilateral derivatives on Bitcoin whose payout is fixed by an oracle signature, with the terms of the contract invisible on chain; grassroots currencies share the bilateral form and settle with no chain—a transaction is a swap between the two parties, enforced by the written obligations of the coins rather than by a spending transaction. The generalised state-channel frameworks [18,24] run arbitrary contracts off chain between two parties and keep the chain as the adjudicator of last resort; a grassroots coin has no such adjudicator, and a party who disowns their signature is in default, remedied at law and made public by the record (Section 5.2).

Monetary theory. Grassroots currencies create *inside money* [14,15]—a medium of exchange backed by private credit rather than sovereign authority. Cavalcanti and Wallace [15] studied a population of bankers and nonbankers: bankers' financial histories are public, enabling punishment for deviation, while nonbankers' histories are private, making notes an essential medium of exchange. In grassroots currencies, everyone is between a banker and a nonbanker: financial records are not public, but the holder of another person's coins can choose which coin to redeem against it among those held by the other person, requiring the coin holder to have access to such knowledge.

Kocherlakota's result that "money is memory" [52] is directly relevant: grassroots currencies replace monetary tokens with cryptographic records of bilateral obligations, with agents holding the distributed memory that makes money possible. The Bank of England's account of how commercial banks create money through lending [62] describes a process structurally analogous to the opening of a mutual credit line: in both cases, the act of lending simultaneously creates both an asset (the loan) and a liability (the deposit or coin). The theoretical foundation for such endogenous money creation through credit is established by Palley [68]. Brunnermeier et al. [11] provide a comprehensive framework connecting inside/outside money, token/account forms, and digital currency competition, within which grassroots currencies occupy a distinctive position as peer-issued, record-based inside money operating without either sovereign backing or blockchain consensus. Finally, Mundell's theory of optimum currency areas [66] is relevant to the regional bank and currency recognition mechanisms of Appendix E, which allow grassroots currency areas to form and merge bottom-up rather than top-down.

Motivation and limitations. Grassroots currencies are for communities in which people already trust each other—families, neighbours, colleagues, a community bank and its members—as a credit line is opened only between persons willing to hold each other's debt. Among strangers no such line is opened, so the currencies form where trust already is, and reach further along the chains of Section 2. Without a shared ledger no person sees total issuance: each sees the coins they hold, and the holdings that friends disclose to each other, from which the ratio of Section 2.4 is computed. An estimate of a counterparty's default is thus as good as their disclosure. A currency per person makes the number of currencies the number of persons; the holdings of each person are the currencies of the few they trade with, so the record a person keeps grows with their own circle and not with the economy.