Cash Transfer Primitives, Trust and Money

Javier Thayer
Joshua Guttman

Outline and Purpose of Talk

- Apply trust management to electronic finance.
- Consider financial primitives
  - $\mathbf{transfer}(A_1, A_2, p, N)$,
  - $\mathbf{debit}(A_1, p, N)$,
  - $\mathbf{credit}(A_2, p, N)$
  - Other primitives to reverse transactions.
- Protocol aggregation assurances
  - Global reliability properties.
  - Measurable effects on monetary aggregates

Motivation

- An electronic financial system consists of many interacting protocols
- The relation to each other is protocol mixing problem
- The structure of financial environment can suggest other properties beyond authentication.
- Provide an interface between protocol and financial environment.

EPMO Protocol

$$
\begin{tikzcd}
B & & C & & M \\
& & n_{c,1} \arrow[rr, "\{\!|C \frown N_c \frown \mathsf{goods} \frown \mathsf{price}|\!\}_M"] \arrow[d, Rightarrow] & & n_{m,1} \arrow[d, Rightarrow] \\
& & n_{c,2} \arrow[d, Rightarrow] & & n_{m,2} \arrow[ll, "\{\!|N_c \frown N_m \frown M \frown \mathsf{goods} \frown \mathsf{price}|\!\}_C"'] \arrow[ddd, Rightarrow] \\
n_{b,1} \arrow[d, Rightarrow] & & n_{c,3} \arrow[ll, "\{\!|C \frown N_c \frown N_m \frown \mathsf{price}|\!\}_B"'] \arrow[d, Rightarrow] & & \\
n_{b,2} \arrow[rr, "\mathsf{mo} \frown \{\!|N_c \frown N_b|\!\}_C"] \arrow[dd, Rightarrow] & & n_{c,4} \arrow[d, Rightarrow] & & \\
& & n_{c,5} \arrow[rr, "\mathsf{mo} \frown N_b"] & & n_{m,3} \arrow[d, Rightarrow] \\
n_{b,3} & & & & n_{m,4} \arrow[llll, "\llbracket\, \mathsf{hash}(B \frown N_b \frown N_m)\, \rrbracket_M"']
\end{tikzcd}
$$

Economic Transaction

- Transfer of funds between accounts.
- Creating claims to assets (or services).
  - transfer occurs when bank receives transfer request
- Financial institutions guarantees balances, transfer of balances etc.

History

- Linear history: finite or infinite sequence of oriented formulas.
  - positive is guarantee,
  - negative is rely.
- A global history is a set of linear histories.
- Embedding of a linear history h into a strand s is a monotone preserving mapping of h into s which preserves sign of nodes.
- Realization of a set of oriented histories by bundle over annotated protocols.

Financial Model

- An *account* is some structure $A \in \mathbf{Account}$
  - prin(A) is owner
  - bank(A) is resident bank.
  - A has a state space Ω_A.
- Banks $B \in \mathbb{B}$
  - $\mathbb{B}$ is rooted tree.
  - Banks are principals.
  - Bank has an account with itself and an account in the parent bank.

Financial Model

- A *financial theory* contains primitives such as $\mathbf{transfer}(C, M, p, N)$, $\mathbf{debit}(C, p, N)$, $\mathbf{credit}(M, p, N)$ together with some formulas such as

$$\mathbf{transfer}(C, M, p, N) \wedge (p \leq \mathsf{balance}(C))$$

$$\Longrightarrow$$

$$\mathbf{debit}(C, p, N) \wedge \mathbf{credit}(B, p, N)$$

  provided $\mathsf{bank}(C) = \mathsf{bank}(M)$.

  – N is a transaction identifier.

Financial Model

- If $\mathsf{bank}(A) \neq \mathsf{bank}(B)$,

$$\mathbf{transfer}(C, M, p, N) \wedge (p \leq \mathsf{balance}(C))$$

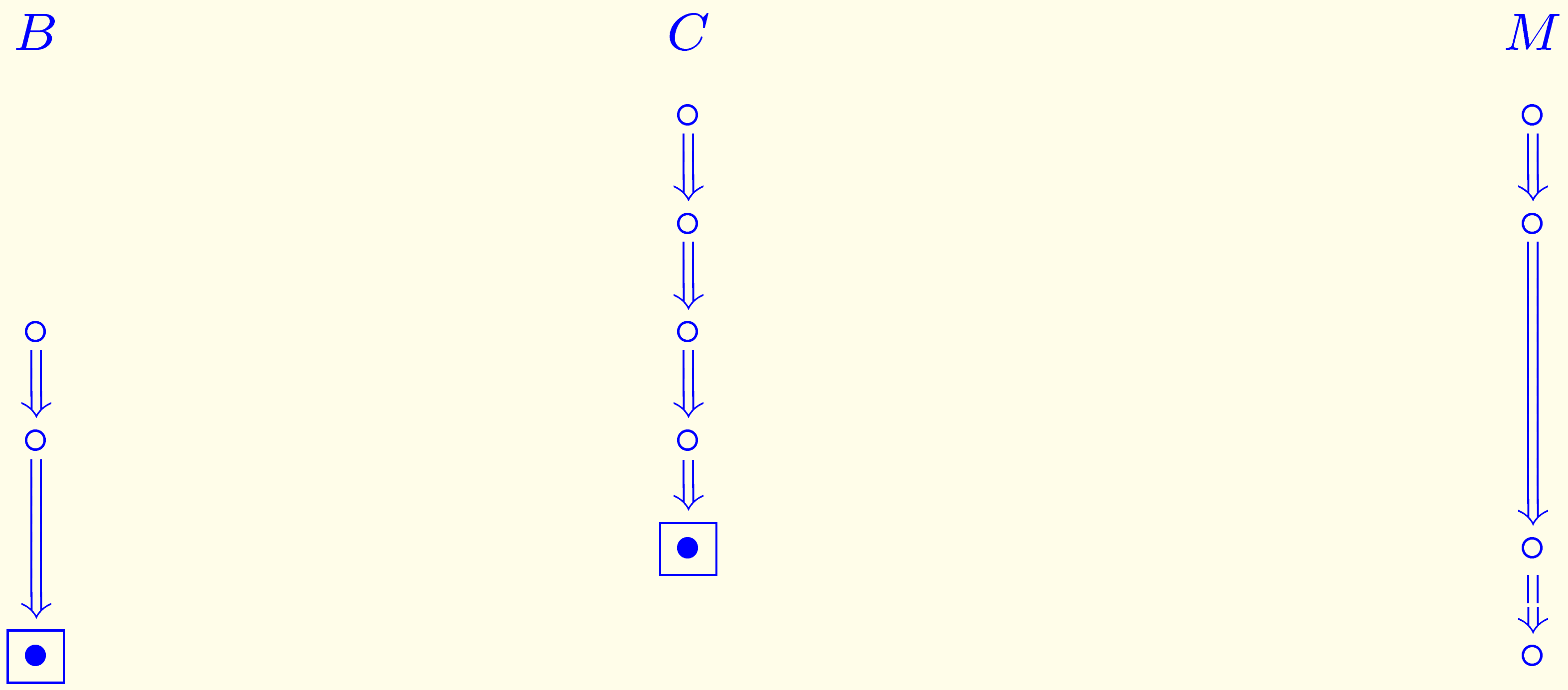
$$\Longrightarrow$$

$$\mathbf{debit}(C, p, N) \wedge$$

$$\mathbf{credit}(\mathsf{bank}(C), p, N) \wedge$$

$$\mathbf{transfer}(\mathsf{bank}(C), M, p, N)$$

Financial Events in EPMO



Financial Events in EPMO

$$
\begin{array}{c}
B \\
\\
\\
\circ \\
\Downarrow \\
\circ \\
\Downarrow \\
\boxed{C \text{ says } \mathbf{transfer}(C, M, p, N)}
\end{array}
\qquad\qquad
\begin{array}{c}
C \\
\circ \\
\Downarrow \\
\circ \\
\Downarrow \\
\circ \\
\Downarrow \\
\circ \\
\Downarrow \\
\boxed{\mathbf{transfer}(C, M, p, N)}
\end{array}
$$

Banks Linear Financial History

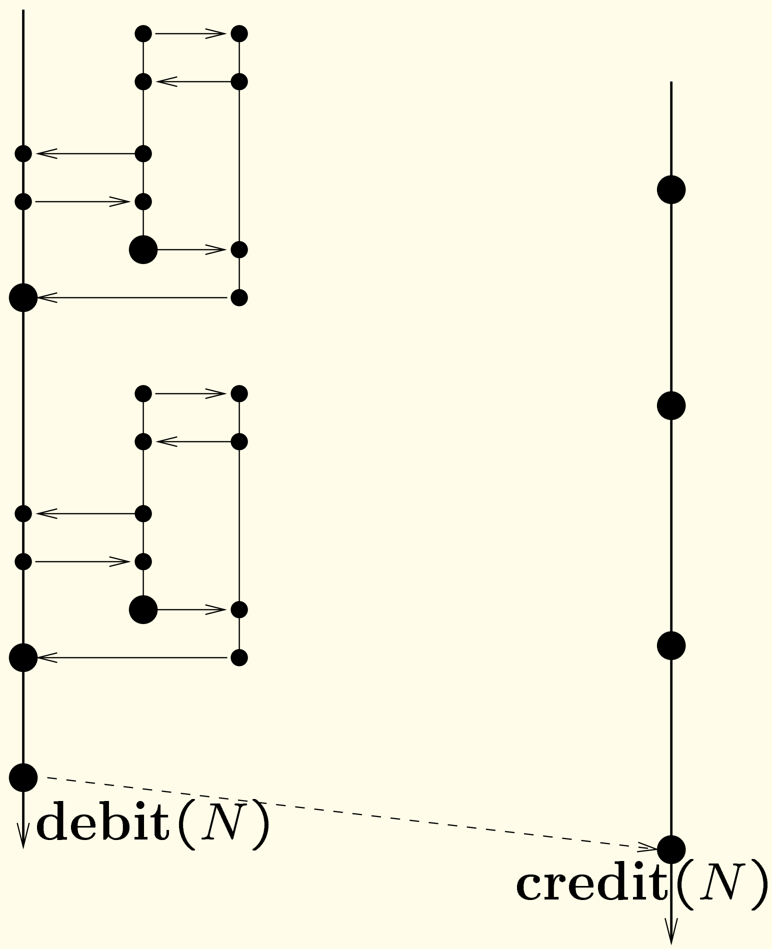
$$B$$

$$\begin{array}{c} \circ \\ \Downarrow \\ \circ \\ \Downarrow \\ \boxed{C \ \textsf{says}\ \mathbf{transfer}(C, M, p, N)} \\ \Downarrow \\ \boxed{\mathbf{transfer}(C, M, p, N)} \\ \Downarrow \\ \boxed{\mathbf{debit}(C, p, N) \wedge \mathbf{credit}(M, p, N)} \end{array}$$

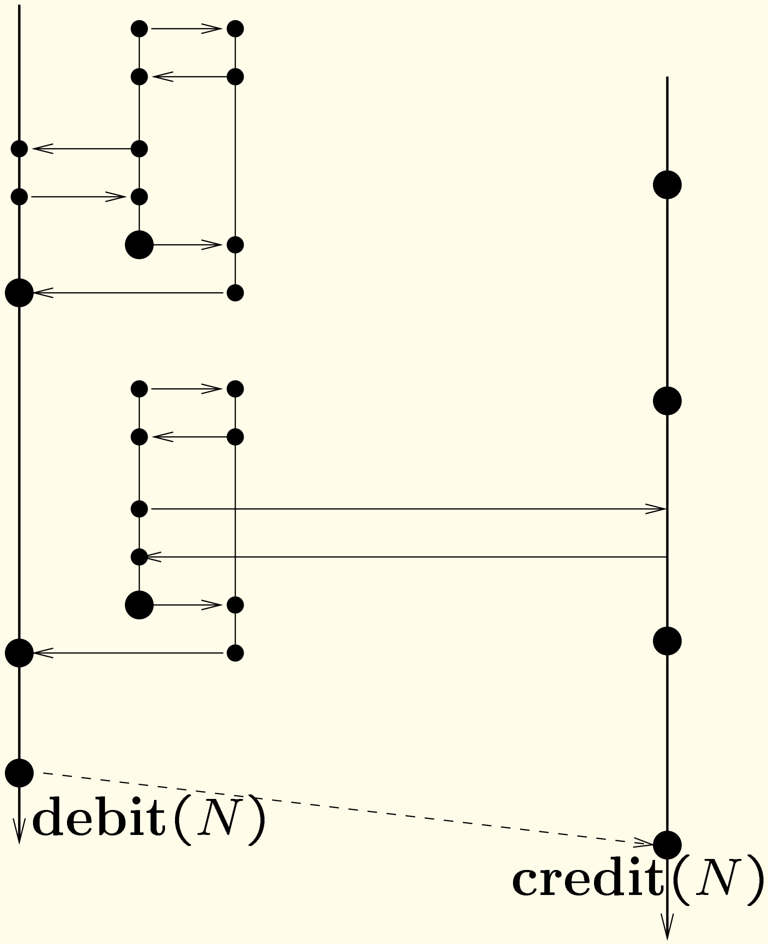
Double Entry Graph

$$\begin{tikzcd}
\text{Account } A \arrow[d, Rightarrow] & & \text{Account } M \arrow[dd, Rightarrow] \\
\boxed{\mathbf{debit}(C, p, N)} \arrow[dd, Rightarrow] & & \\
& & \boxed{\mathbf{credit}(M, p, N)} \arrow[d, Rightarrow] \\
{} & & {}
\end{tikzcd}$$

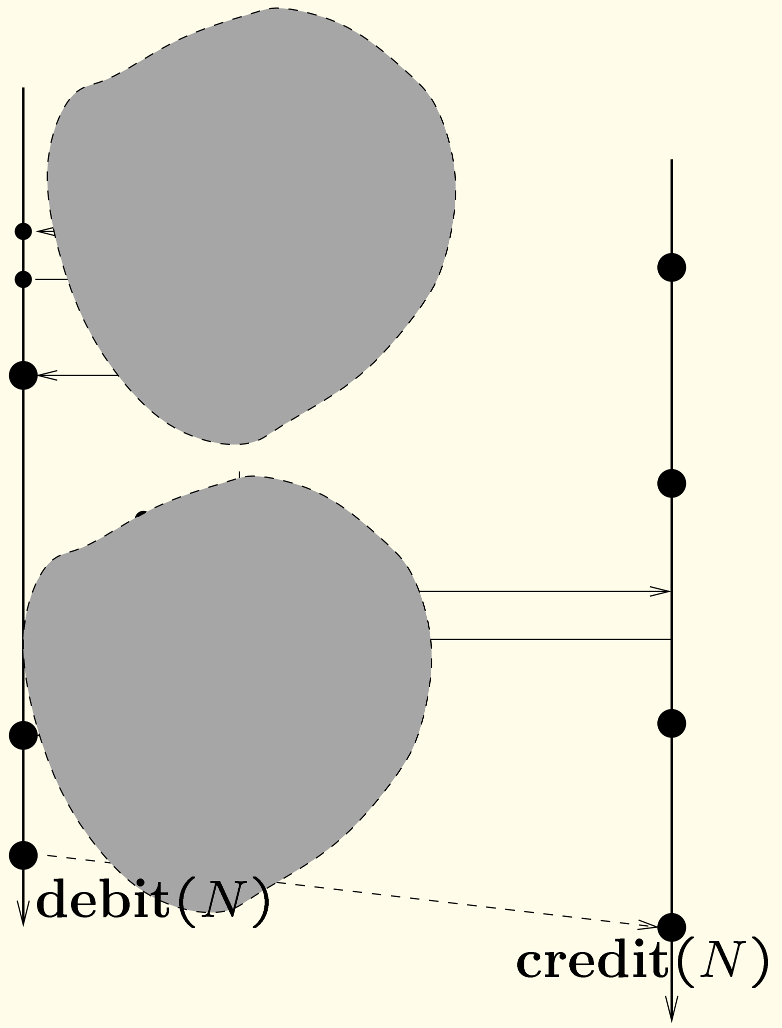
Banking Transactions



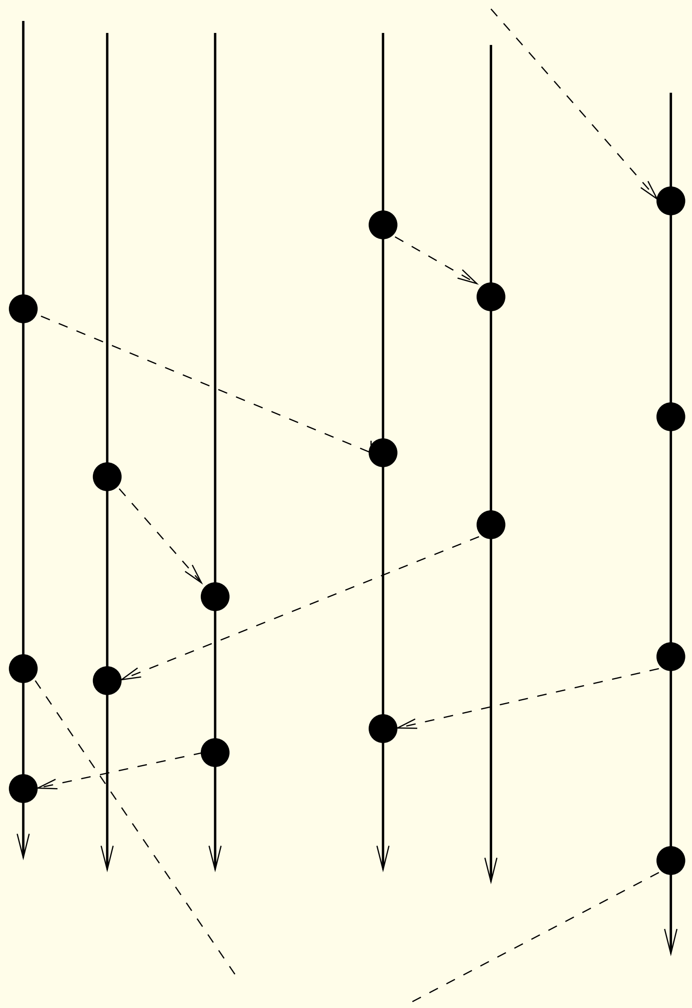
Banking Transactions



Banking Transactions



Flows



Conservation of Money

- M_μ = Balance at μ.
- Outflows $= \sum_{\mu \preceq \lambda \preceq \nu} \mathbf{debit}(A, p(\lambda), n(\lambda))$.
- Inflows $= \sum_{\mu \preceq \lambda \preceq \nu} \mathbf{credit}(A, p(\lambda), n(\lambda)) + M_\mu$.
- Inflows $-$ Outflows ≥ 0.

Failures

- Simple accounting failures:
  - Expenses beyond budget
  - A debit with no credit or vice versa.
- Protocol Failure
  - Rely A says $\textbf{transfer}(A, B, p, N)$ without guarantee $\textbf{transfer}(A, B, p, N)$
- Insider Fraud
  - Guarantee $\textbf{transfer}(A, B, p, N)$ without Rely A says $\textbf{transfer}(A, B, p, N)$

Monetary Flows

Let G be a directed loopless graph.

- *currency flow* in G is a map $d : \text{edges}(G) \to \mathbb{N}$ such that for every $x \in \text{nodes}(G)$,

$$\sum_{\text{target}(v)=x} d(v) = \sum_{\text{source}(v)=x} d(v).$$

- $A \subseteq \text{nodes}(G)$ is *invariant* iff $x \in A$ and $x \longrightarrow y$, then $y \in A$.
- A is *reducing* iff both A and $\complement A$ are invariant.
- G is *completely reducible* iff every invariant set is reducing.
- G is *irreducible* iff it has no invariant subsets.

Irreducibility

- G is irreducible iff for every $x, y \in \text{nodes}(G)$, there is a path $x \longrightarrow^{+} y$.

Proof. If there is no path $x \longrightarrow^{+} y$, then the set of $z \in \text{nodes}(G)$ such that $x \longrightarrow^{+} z$ is invariant and does not contain y. Conversely, if there is some proper invariant subset A, and $x \in A$, $y \in \complement A$, there is no path $x \longrightarrow^{+} y$. ■

Existence of Currency

- A finite irreducible graph G has a currency flow.

Proof. Let $d(v) = \text{card}\{\text{cycles containing } v\}$. By irreducibility, v is contained in at least one cycle. ■

Leontiev Models of Currency Flows

- A is an indecomposable matrix "of intersectorial cash flows", x is the per-sector quantity of money
- Currency flows satisfy

$$x = Ax$$

- Price level associated eigenvector of dominant eigenvalue.

Conclusion

- Lenin is said to have declared that the best way to destroy the capitalist system was to debauch the currency. (J. M. Keynes)

- Even with “paper receipts for transactions”, nature of currency will eventually be tightly woven with operation of large numbers of protocols.

- Quantitative measurements on relevant financial variables.