Self-Recharging Virtual Currency

David Irwin, Jeff Chase, Laura Grit,

and Aydan Yumerefendi

Department of Computer Science
Duke University

Motivation

Networked computing utilities have matured

- E.g., content service networks, computational grids, application hosting services, network testbeds

Need better solutions to manage shared resources

- “Tragedy of commons” apparent to any PlanetLab user

Market-based control is a logical next step

- Grid deployments reaching level of scale where market-based control is necessary
- Recent practical examples encouraging
    - E.g., BitTorrent incentives engineered to induce global behavior

Cereus

- Market-based system for resource sharing
  - Lease raw hardware resources to ***community*** of consumers
    - Foundation is SHARP [fu03]
  - Introduce ***common currency*** with exchanges brokered by 3rd parties
- Community vs. Peer-to-Peer
  - Community - Users authenticated and bound to identities
    - Makes accountability possible
  - P2P - Anonymous users; scales well
    - Consumption = Contribution
- Communities applicable in many situations
    - E.g. PlanetLab, Grids, Corporations, Campus networks

Cereus introduces a common currency

Currency usage in Cereus is accountable

- Users may cheat and overspend currency
  - But cheaters are caught/punished

Transactions subject to audit

- Occur off-line and “after-the-fact”
- Suitable in community environment where:
  - Users not anonymous
  - Faithfulness dominates privacy
  - Resource providers are selfish but not malicious
- Audits do not require trust

Controlling Resource Sharing in Cereus

Cereus has ***producers*** and ***consumers***

- Roles are separate

  Producers receive currency in exchange for resources

  Consumers receive resources in exchange for currency

- E.g., producers cannot use currency earned from sales to buy

Community should control currency

- Resources benefit community

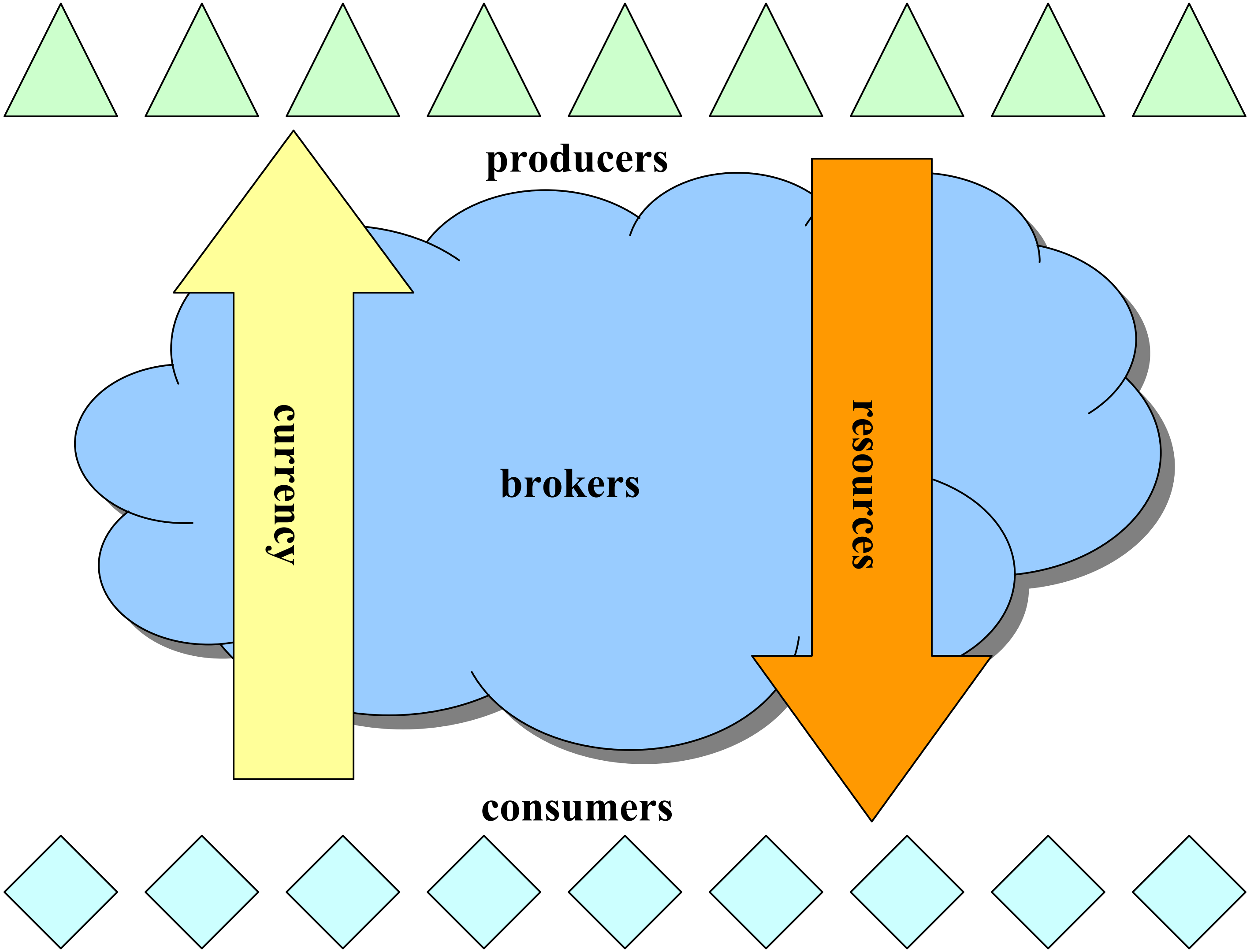
  And distribution of currency determines resource allocation

- Cereus **does not** specify how currency distributed (pluggable policy)

  Could be Consumption = Contribution or cash payment

Cereus uses *virtual currency* (called credits)

Overview of a Cereus Community



producers

currency

brokers

resources

consumers

Cereus Credits are Self-Recharging

How do we recycle virtual currency?

- Money economies have trouble if Consumption ≠ Contribution

  Require an allowance; users may hoard or starve

- ***Self-recharging currency reverts to the users budget after some delay***

  Ensures stable budget

  Avoids complicated recycling mechanisms

Not a new idea

- Lottery scheduling

  Currency reverts immediately

- Credits derived from [Sutherland68]

  Currency reverts after consumption

Outline

- Overview
  - Motivation
  - Cereus
- Currency Management
  - Sutherland’s PDP-1 Market
  - Generalizing the PDP-1 Market
  - Credits vs. Money
- Currency Design
  - Credits and SHARP claims
  - Auditing
- Related Work and Conclusions

Sutherland's PDP-1 Market

Self-recharging currency introduced by [Sutherland68]

- Widely cited paper; used "yen" to access PDP-1

  Open-ascending english auction on public board

Market Rules:

- Bidding period determines allocation for next day (24 hours)

  E.g., Bid on Tuesday for usage on Wednesday

- Bidders commit currency when bid placed (write on board)

  Currency immediately available to bidder if bid preempted

- Market recharges currency after resource consumed

Generalizing the PDP-1 Market

Extend PDP-1 market to:

- Networked multi-actor market
- Multiple, multi-unit, continuous, rolling, brokered auctions

When to recharge credits spent for winning bids?

- PDP-1 recharges after resource consumed
- Insufficient for continuous rolling auctions
    - Dominant strategy to bid for instant gratification (credits recharge sooner)
    - Reverts to proportional share
- Effect negated in PDP-1
    - Buyers always receives credits before next bidding period

Solution: maintain consistent recharge time

Credit Recharge Rule

Rule: *spent credits recharge fixed interval after bid placed*

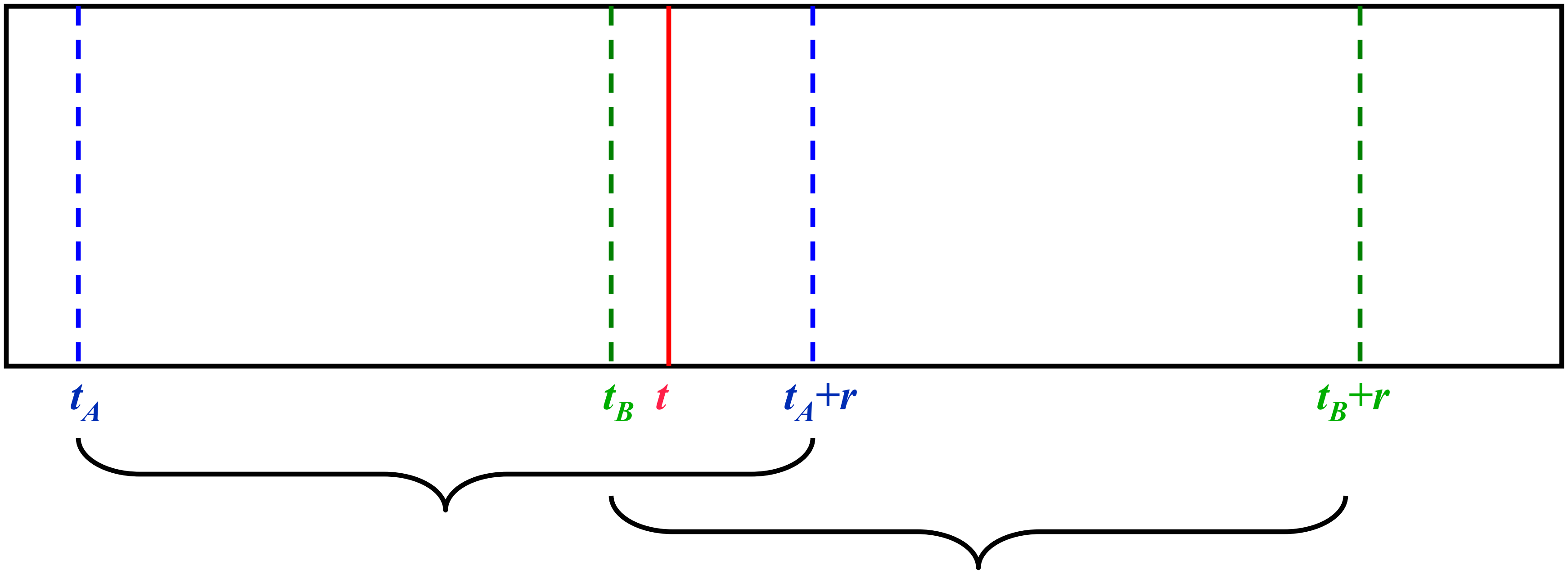
- Recharge time is global property of system
- Never spend more than budget over any recharge time interval

Benefits

- Encourages early bidding
    - Yields more accurate price feedback to bidders
    - Discourages predatory late bidding before auction closes
- Discourages canceled bids
    - Shifting credits to another bid delays recharge
- Encourages early bidders to bid higher
    - Avoids incurring opportunity cost on credits for losing bids

Credit Recharge Rule

A commits credits at t_A
B commits at t_B → Auction for resources at time t → *A*'s credits recharge sooner than *B*'s



recharge time = r

Binding Bids Rule

Implications for brokered auctions

- Credits passed to broker expire to preserve currency balance
- Brokers have incentive to spend credits quickly

Rule: *credits committed to bid become unavailable until recharge*

- Simplifies currency management
- Bidders cannot cancel/reduce bids

  Result: brokers need not return escrowed credits after being spent

- Brokers are pure middle-men

  Cannot: accumulate credits, go into deficit, or hold working capital

Cereus Credits vs. Money

Adjustable incentives to conserve/plan over time

- Credits bound hoarding and starvation
  - May spend credit budget in any recharge time interval
- With a short recharge time:
  - Similar to proportional share; no need to conserve
- With a long recharge time:
  - Resembles money economy; must conserve currency/plan usage

In perfect markets:

- Consumers assured access to share of resource value proportional to share of wealth
- **With credits:** assurance applies to any recharge time interval

Holding Users Accountable in Cereus

Self-interested users may lie/cheat/steal

- Attempt to spend currency before recharge time
- May overspend currency
- **Possible solution:** coordinate all transactions through bank

Credits offer simple/enforceable decentralized alternative

- Verifiable time element
    - Credit transfers have expiration time; users must delay recharges
- **Cereus solution:** currency transfers occur without bank interaction

Recharge rule and binding bids rule make it possible to represent credits as chains of SHARP claims

Cereus Currency Design

Credits formed using SHARP abstraction of *accountable claim*

- Called *credit notes*
  - Similar to other SHARP claims (*lease/tickets*)
- Digitally signed, time-stamped assertion of ownership
  - SHARP supports secure delegation of claims
- Bank service authenticates users and issues budgets
  - Users recharge locally; bank not involved in transfers

Currency actions held accountable

- Auditors detect misbehavior
- Provable and non-repudiable

Auditing in Cereus

Credits pass up chain of intermediary brokers

- All tickets for resources/credit notes end up at sites
- Includes all information to detect/prove misbehavior
  - Mechanisms described in [fu03]

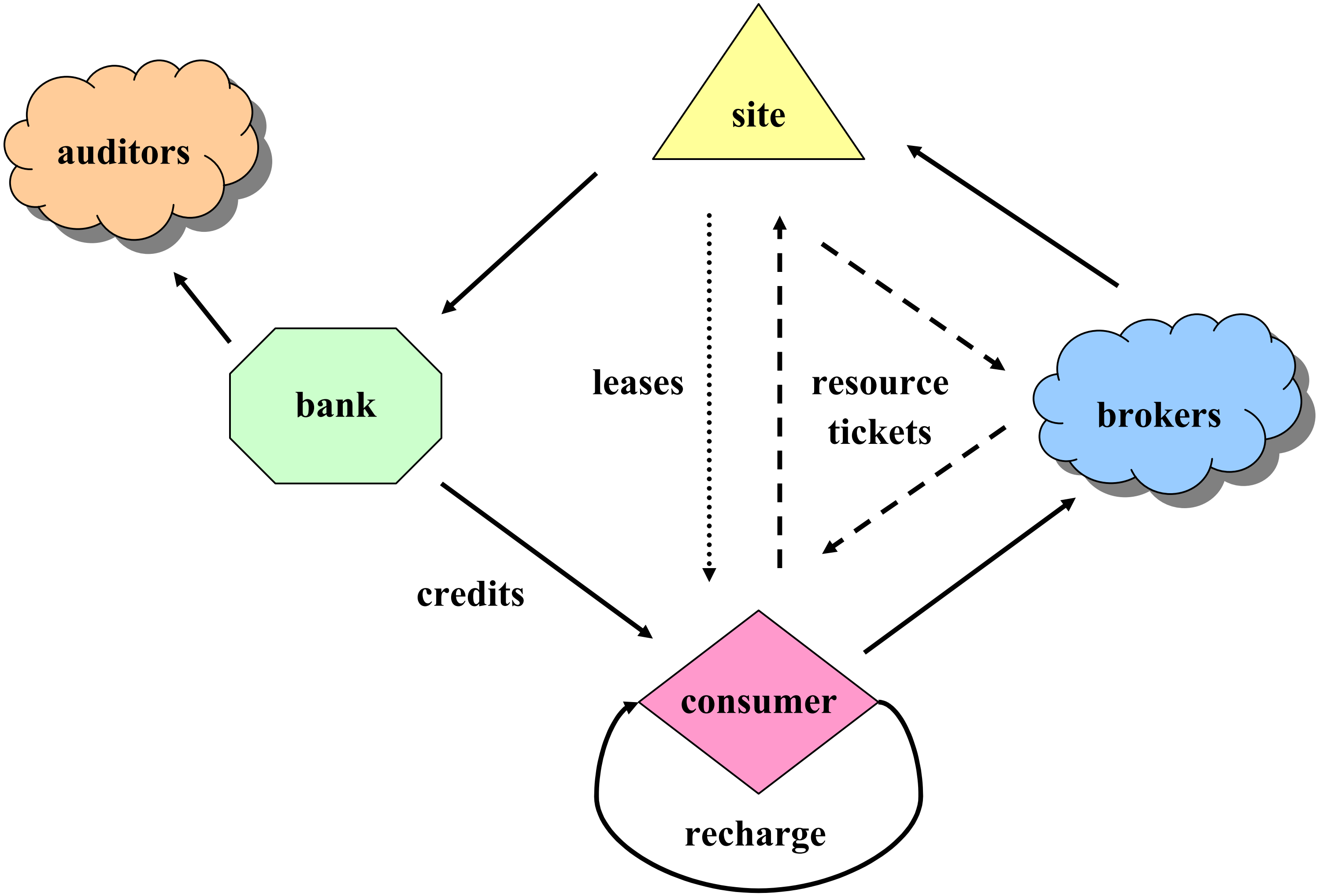
Incentive for sites to provide credit notes to auditors

- Provide willingly; proof of value to community

Other issues

- Auditors need not be trusted
  - Collusion must be prevented
- Probabilistic sampling may be employed
  - Tradeoff detection accuracy and performance
- Audits not privacy preserving
  - May encrypt predecessor credit notes with bank's public key

Cereus Credits/Resource Cycle



Cereus Prototype

Prototype Implementation

- ~18000 LOC
- Includes:
  - Reservation manager
  - Plug-in resource manager (currently uses COD)
  - Plug-in crypto package
  - Plug-in bidding/auction policies

Cluster-On-Demand (COD)

- Resources: physical machines or Xen
  - May run in real or emulated setting

Related Work

Peer-to-Peer

- Anonymous users; trust by reputation
  - E.g., Karma, SWIFT, CompuP2P
- Consumption = Contribution

Industry initiatives

- Use cash instead of virtual currency
- Asynchronous accountability mechanisms not possible

Virtual currencies

- Some markets assume single trust domain
- Closely related to Tycoon (HP)
  - Cereus based on a leasing abstraction

Conclusion

Cereus uses *virtual currency*

- Community controls allocation of currency
- External sources have no power to subvert policy choices

Propose self-recharging currency for *community* resource sharing

- Enables *distributed currency management*
  - Resource sharing is accountable
- Avoids complicated recycling mechanisms
  - Configurable tradeoff b/t proportional share and money economy

Accountable credit management provides strong foundation

- Layer more complex policies and protocols
- Define rules/incentives to induce desired behaviors

Questions