Certified E-mail for Contracts of Changeable Values

[Speaker]

Kenji Imamoto, Kouichi Sakurai

Kyushu University

http://itslab.csce.kyushu-u.ac.jp/

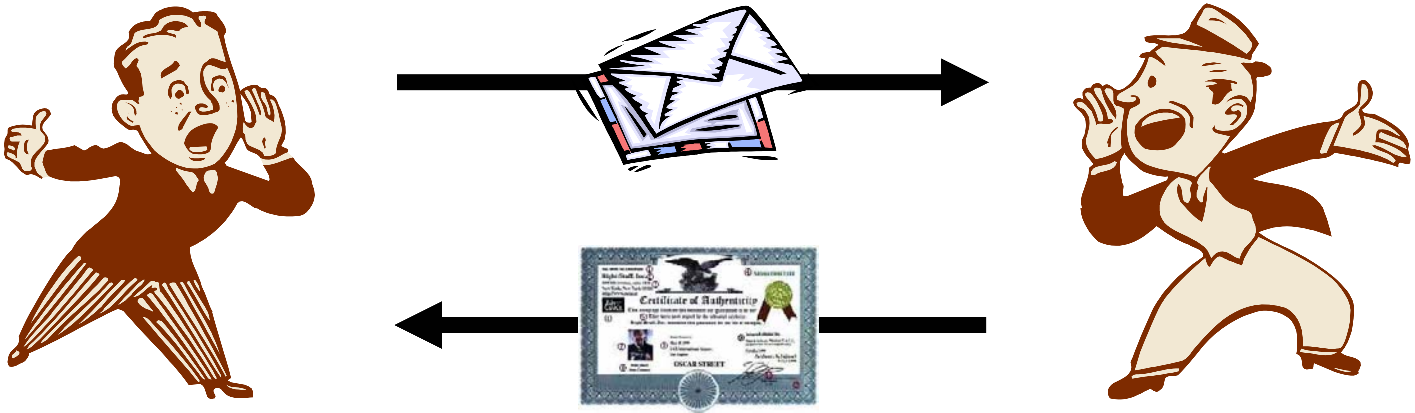
Certified E-mail

- Certified E-mail is a system which enables a sender prove a receiver's receipt of e-mail

Fair Exchange of E-mail and Receipt

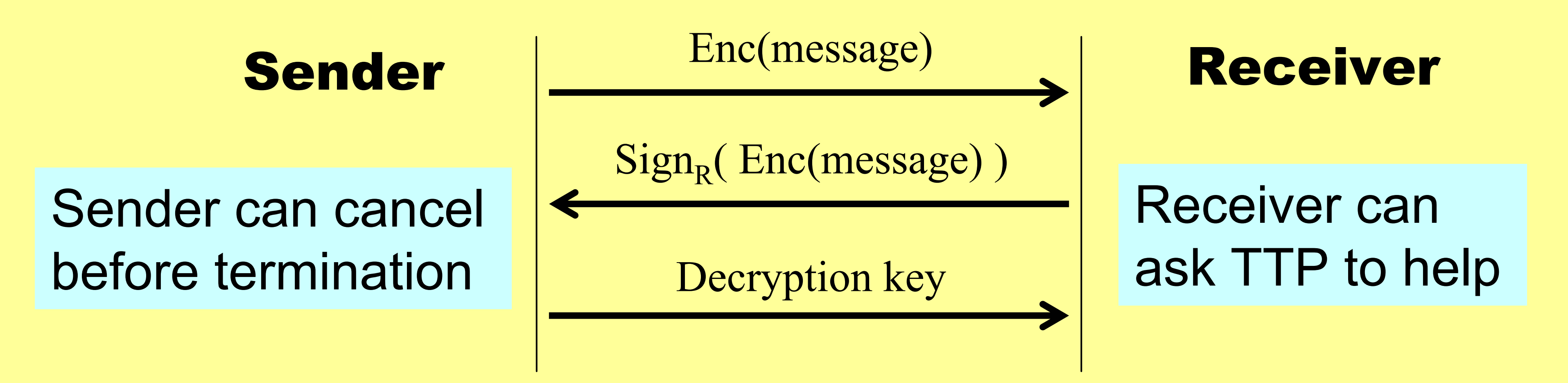
- Fairness
  - – Both parties can obtain his/her desired item, or neither one does

➔ Distribution of Digital Contents, Casino, Voting System, …



Existing Protocol [OZL04]

- The certified e-mail protocol presented in [OZL04]
  - Provides Fairness
    - Use TTP to provide fairness in case of emergency (Optimistic protocol)
  - Provides Timeliness
    - Any participants can terminate a session in finite time without loss of fairness

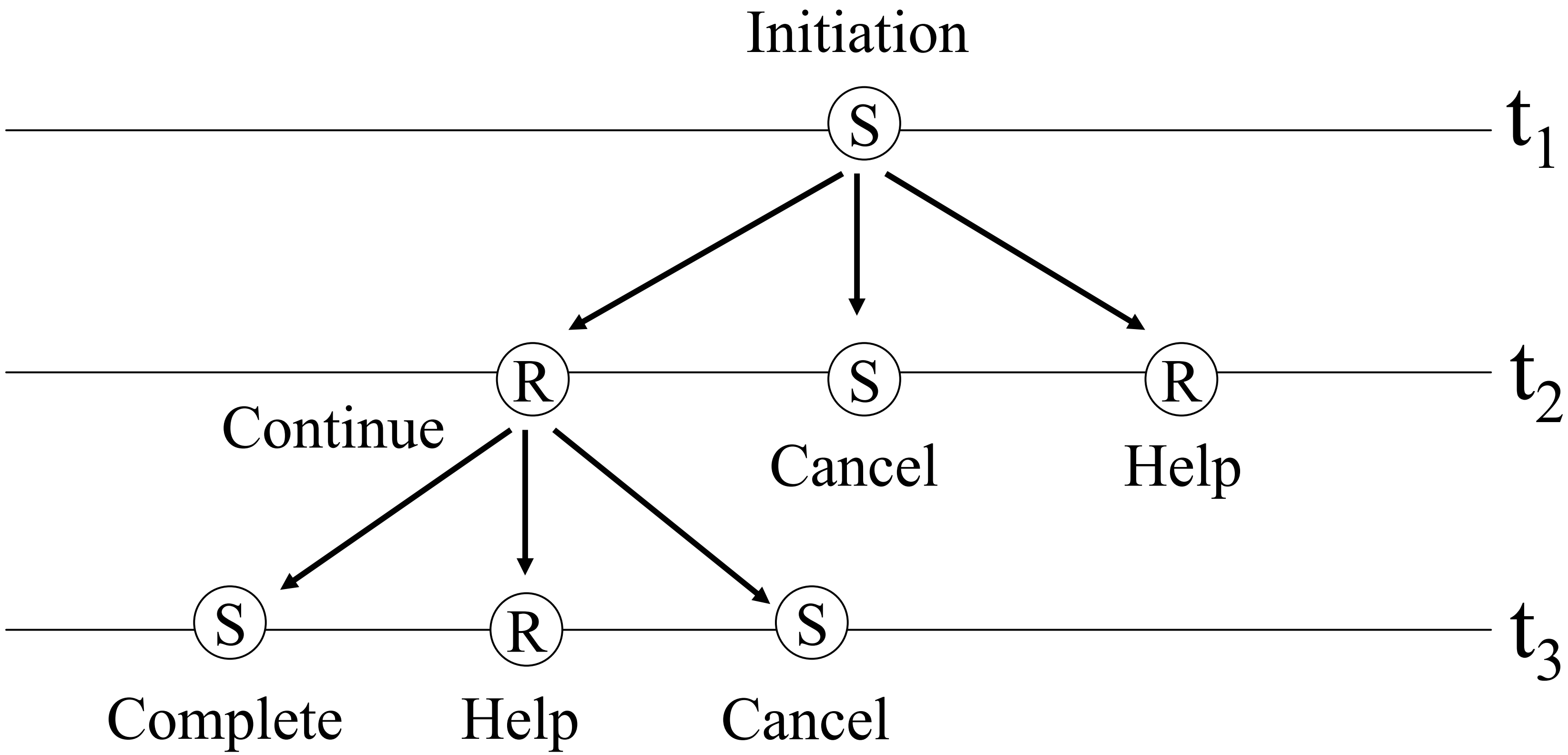


Sender can cancel before termination

Receiver can ask TTP to help

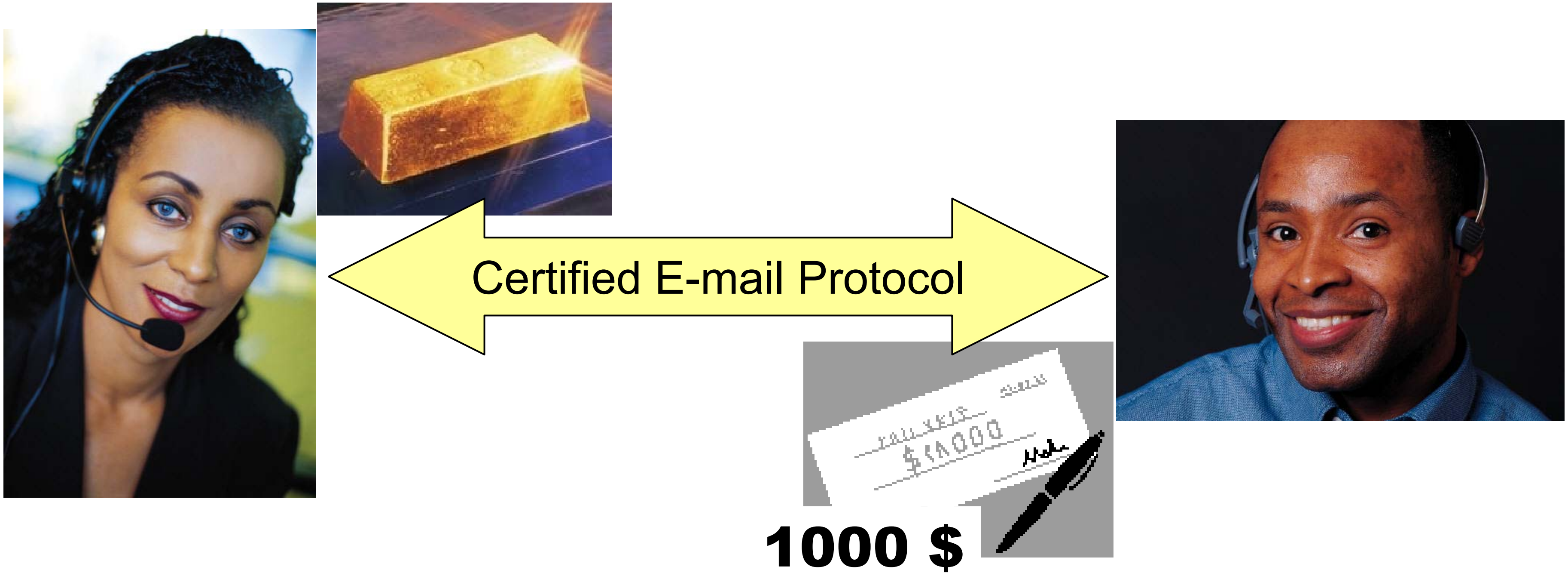
[OZL04] J.A.Onieva, J.Zhou, and J.Lopez, ``Enhancing Certified Email Service for Timeliness and Multicasting'', INC'04.

The Choices of Each Stage [OZL04]

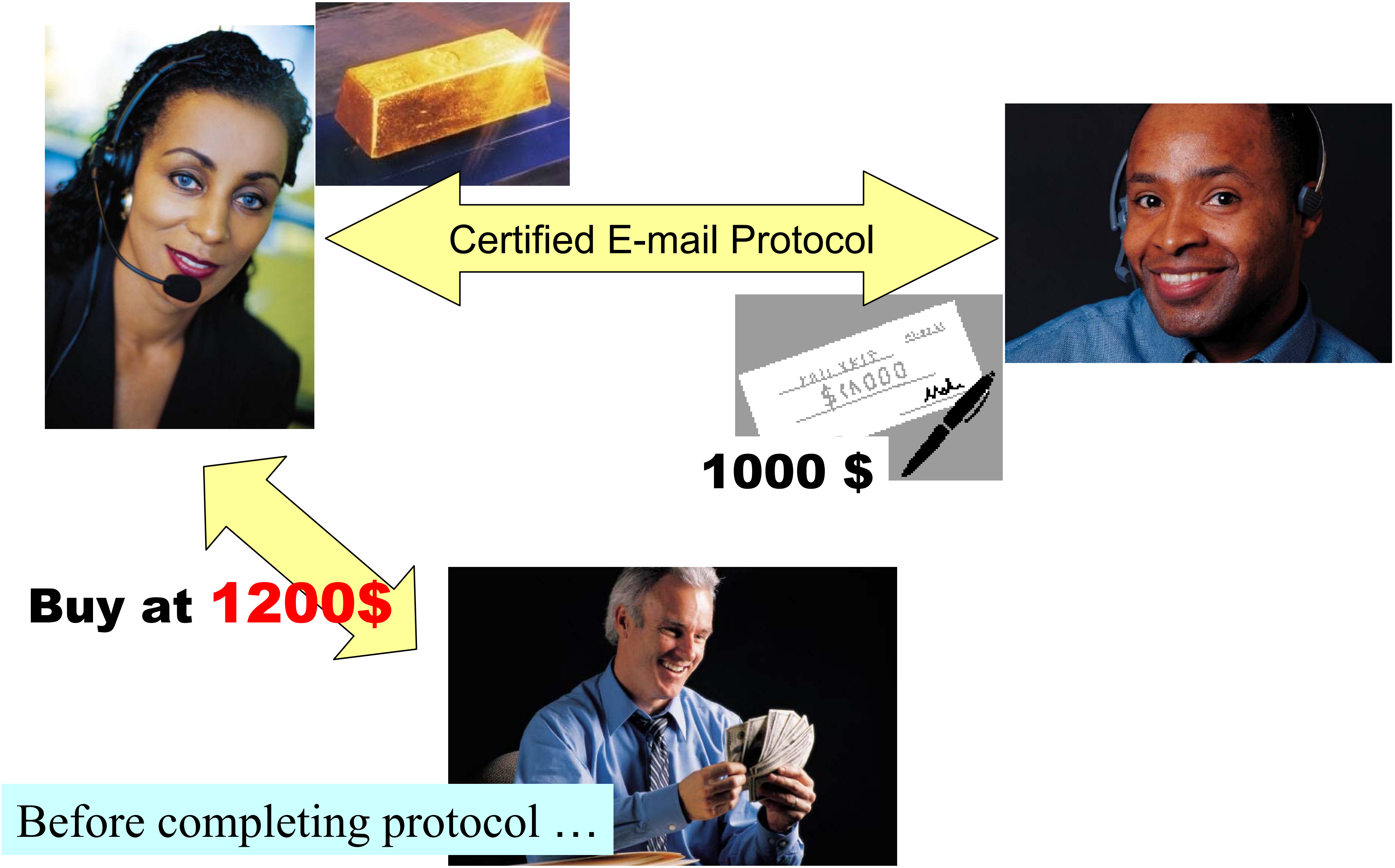


- Sender can change her choice before completing
- After Receiver decided to continue, he cannot refuse
  - Resolution may change during a session …
    - E.g. a stock trade, auction, a kind of soccer pool

Example of Contract by [OZL04]



Example of Contract by [OZL04]



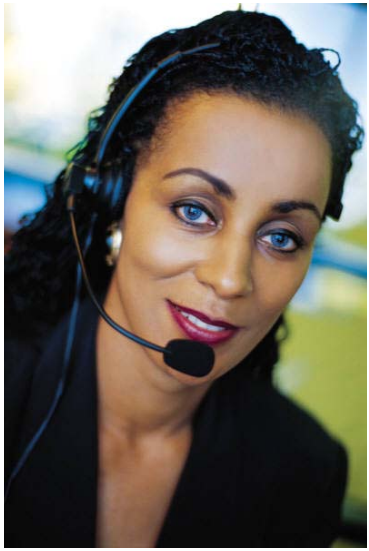
Certified E-mail Protocol

1000 $

Buy at **1200$**

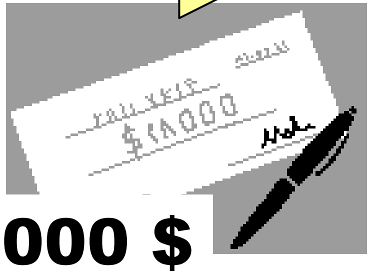
Before completing protocol …

Example of Contract by [OZL04]



Bob cannot change his choice

Certified E-mail Protocol

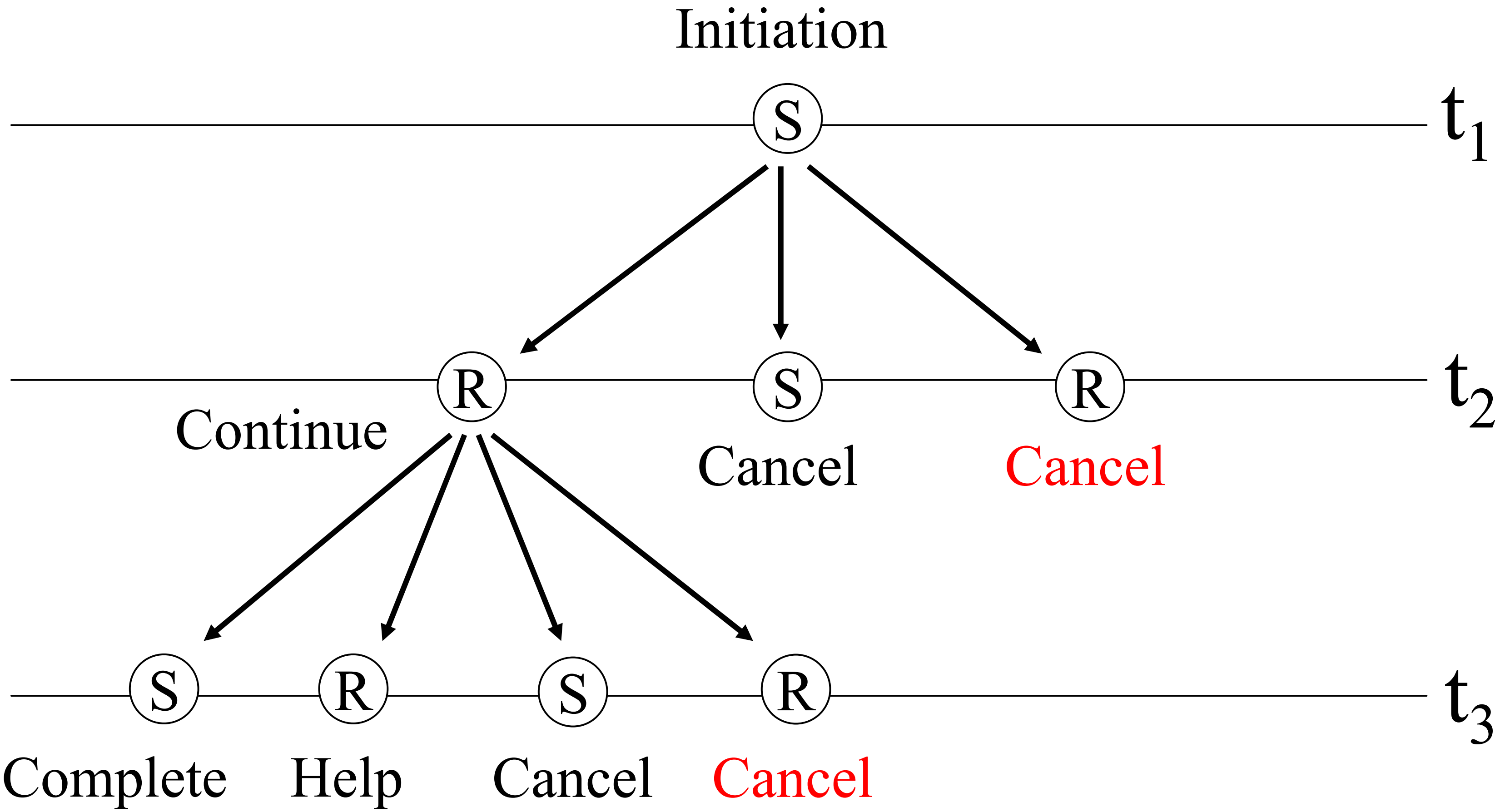


1000 $

Sell off at 800$

After Bob’s no return point …

The Choices of Each Stage
[Proposed Protocol]



Each participant can change his/her choice anytime before a termination without loss of fairness

Work in Progress

- Concretely define evenhanded situations/stages
  - Express behaviors of protocol participants by using Game Theory
    - Expected payoff of each participant should be same
- Design a practical evenhanded protocol under realistic setting